A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension

Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang
(with an appendix by Tim and Vladimir Dokchitser)

March 2, 2017

1 Introduction

In this article, for any fixed genus $g \geq 1$, we prove that a positive proportion of hyperelliptic curves over $\mathbb{Q}$ of genus g have points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all p, but have no points globally over *any* extension of $\mathbb{Q}$ of odd degree.

By a hyperelliptic curve over $\mathbb{Q}$, we mean a smooth, geometrically irreducible, complete curve C over $\mathbb{Q}$ equipped with a fixed map of degree 2 to $\mathbb{P}^1$ defined over $\mathbb{Q}$. Thus any hyperelliptic curve C over $\mathbb{Q}$ of genus g can be embedded in weighted projective space $\mathbb{P}(1,1,g+1)$ and expressed by an equation of the form

$$C : z^2 = f(x,y) = f_0 x^n + f_1 x^{n-1} y + \cdots + f_n y^n \tag{1}$$

where $n = 2g+2$, the coefficients f_i lie in $\mathbb{Z}$, and f factors into distinct linear factors over $\bar{\mathbb{Q}}$. Define the height $H(C)$ of C by

$$H(C) := H(f) := \max\{|f_i|\}. \tag{2}$$

Then there are clearly only finitely many integral equations (1) of height less than X, and we use the height to enumerate the hyperelliptic curves of a fixed genus g over $\mathbb{Q}$.

We say that a variety over $\mathbb{Q}$ is *locally soluble* if it has a point over $\mathbb{Q}_\nu$ for every place ν of $\mathbb{Q}$, and is *soluble* if it has a point over $\mathbb{Q}$. It is known that most hyperelliptic curves over $\mathbb{Q}$ of any fixed genus $g \geq 1$ when ordered by height are locally soluble (cf. [27] and [3], where it is shown that more than 75% of hyperelliptic curves have this property).

The purpose of this paper is to prove the following theorem.

Theorem 1. *Fix any $g \geq 1$. Then a positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ of genus g have no points over any odd degree extension of $\mathbb{Q}$.*

Let $J = \mathrm{Pic}^0_{C/\mathbb{Q}}$ denote the Jacobian of C over $\mathbb{Q}$, which is an abelian variety of dimension g. The points of J over a finite extension K of $\mathbb{Q}$ are the divisor classes of degree zero on C that are rational over K. (When C is locally soluble, we will see that every K-rational divisor class on C is represented by a K-rational divisor.) Let $J^1 = \mathrm{Pic}^1_{C/\mathbb{Q}}$ denote the principal homogeneous space for J whose points correspond to the divisor classes of degree one on C. A point P on C defined over an extension field $K/\mathbb{Q}$ of odd degree k gives a rational point on J^1, by taking the class of the degree-one divisor that is the sum of the distinct conjugates of P minus $(k-1)/2$ times the hyperelliptic class d obtained by pulling back $\mathcal{O}(1)$ from $\mathbb{P}^1$. Thus Theorem 1 is equivalent to the following:

Theorem 2. *Fix any $g \geq 1$. For a positive proportion of locally soluble hyperelliptic curves C over $\mathbb{Q}$ of genus g, the variety J^1 has no rational points.*

To prove Theorems 1 and 2, we show that for a positive proportion of locally soluble hyperelliptic curves C over $\mathbb{Q}$, the varieties J and J^1 are not isomorphic over $\mathbb{Q}$. To distinguish these varieties, which become isomorphic over $\overline{\mathbb{Q}}$, we will study their arithmetic fundamental groups. In fact, we need only the quotient of the arithmetic fundamental group given by two-covers.

Let I be a principal homogeneous space for the abelian variety J. A *two-cover* of I is, by definition, an unramified covering $\pi : Y \to I$ by another principal homogeneous space Y for J with the property that

$$\pi(y + a) = \pi(y) + 2a$$

for any $y \in Y$ and $a \in J$. The degree of any two-cover is 2^{2g}.

The simplest example of a two-cover of J is given by the multiplication-by-2 isogeny $J \xrightarrow{2} J$. Another interesting two-cover of J is $J^1 \xrightarrow{2} J^2 \cong J$, where the first map is multiplication by 2 in $\mathrm{Pic}_{C/\mathbb{Q}}$ and J^2 is identified with J by translation by the hyperelliptic class d of degree 2. If $\pi : Y \to J$ is any two-cover of J, then the fiber over the origin gives a principal homogeneous space $Y[2]$ for the 2-torsion subgroup $J[2]$, and the class of this homogeneous space in the Galois cohomology group $H^1(\mathbb{Q}, J[2])$ determines the isomorphism class of the two-cover π.

The two-covers $\pi : Y \to J$ where Y has points over $\mathbb{Q}_\nu$ for all places ν are called *locally soluble*. They correspond to elements in the 2-Selmer subgroup $\mathrm{Sel}_2(J)$ of $H^1(\mathbb{Q}, J[2])$. The 2-Selmer group is finite, and lies in an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}_2(J) \to Ш_J[2] \to 0.$$

The isogeny $J \xrightarrow{2} J$ corresponds to the trivial class in the Selmer group, and the two-cover $J^1 \xrightarrow{2} J^2 \cong J$ gives a class $W[2]$ in the Selmer group whenever C (and hence J^1) is locally soluble. This class turns out to be non-trivial 100% of the time, as points of $W[2]$ correspond to Weierstrass divisors e of degree 1 on C with $2e \equiv d$. These divisors e correspond to odd factorizations of $f(x, y)$ over $\mathbb{Q}$. An *odd* (resp. *even*) *factorization* of $f(x, y)$ over $\mathbb{Q}$ is a factorization of the form $f(x, y) = g(x, y)h(x, y)$ where g, h are odd (resp. even) degree binary forms that are either defined over $\mathbb{Q}$ or are conjugate over some quadratic extension of $\mathbb{Q}$. By Hilbert's irreducibility theorem, such factorizations rarely exist. The class $W[2]$ maps to the trivial class in $Ш_J[2]$ if and only if J^1 has a rational point. Hence as an immediate corollary of Theorem 2, we obtain:

Corollary 3. *Fix any $g \geq 1$. Then a positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ of genus g have nontrivial 2-torsion in the Tate-Shafarevich groups of their Jacobians.*

Remark 4. Another consequence of the fact that odd and even factorizations of a binary form $f(x, y)$ over $\mathbb{Q}$ rarely exist is that for 100% of all locally soluble hyperelliptic curves C over $\mathbb{Q}$, the set $J^1(\mathbb{Q})$ is either empty or infinite. Indeed, if J^1 has a rational point, then the class of $W[2]$ in $H^1(\mathbb{Q}, J[2])$ lies in the image of the group $J(\mathbb{Q})/2J(\mathbb{Q})$. If $f(x, y)$ has no odd or even factorization over $\mathbb{Q}$, then $W[2]$ is nontrivial and $J(\mathbb{Q})[2] = 0$. Therefore, $J(\mathbb{Q})$ has positive rank and hence is infinite, and as a consequence $J^1(\mathbb{Q})$ is infinite.

Similarly, we define the 2-*Selmer set* $\mathrm{Sel}_2(J^1)$ of J^1 as the set of isomorphism classes of locally soluble two-covers $\pi : Y \to J^1$. This finite set is either empty or forms a principal homogeneous space

for the finite group $\mathrm{Sel}_2(J)$. In fact, $\mathrm{Sel}_2(J^1)$ is the set of all elements in the 4-Selmer group $\mathrm{Sel}_4(J)$ which map to the class of $W[2]$ in $\mathrm{Sel}_2(J)$ in the first descent.

When the set $\mathrm{Sel}_2(J^1)$ is empty, the varieties J^1 and J are non-isomorphic, and distinguished by their two-covers. We will prove:

Theorem 5. *Fix any $g \geq 1$. For a positive proportion of locally soluble hyperelliptic curves C over $\mathbb{Q}$, the 2-Selmer set $\mathrm{Sel}_2(J^1)$ is empty.*

Theorem 6. *Fix any $g \geq 1$. When all locally soluble hyperelliptic curves C over $\mathbb{Q}$ of genus g are ordered by height, the average size of the 2-Selmer set $\mathrm{Sel}_2(J^1)$ is at most 2.*

We expect that the average in Theorem 6 is in fact equal to 2, and thus is independent of g. To prove Theorem 6, we will use the theory of pencils of quadrics to construct and count the locally soluble two-covers of J^1.

Our methods also allow us to count elements, on average, in more general 2-Selmer sets. For C a hyperelliptic curve over $\mathbb{Q}$ having hyperelliptic class d, and $k > 0$ any odd integer, define the *2-Selmer set of order k* for C to be the subset of elements of $\mathrm{Sel}_2(J^1)$ that locally come from $\mathbb{Q}_\nu$-rational points on J^1 of the form $e_\nu - \frac{k-1}{2}d$, where e_ν is an effective divisor of odd degree k on C over $\mathbb{Q}_\nu$, for all places ν. Then we show:

Theorem 7. *Fix any odd integer $k > 0$. Then the average size of the 2-Selmer set of order k, over all locally soluble hyperelliptic curves of genus g over $\mathbb{Q}$, is strictly less than 2 provided that $k < g$, and tends to 0 as $g \to \infty$.*

Theorem 7 implies that most hyperelliptic curves of large genus have no K-rational points over all extensions K of $\mathbb{Q}$ having small odd degree:

Corollary 8. *Fix any $m > 0$. Then as $g \to \infty$, a proportion approaching 100% of hyperelliptic curves C of genus g over $\mathbb{Q}$ contain no points over all extensions of $\mathbb{Q}$ of odd degree $\leq m$.*

Corollary 8 allows us to construct many smooth surfaces and varieties of higher degree, as symmetric powers of hyperelliptic curves, that fail the Hasse principle:

Corollary 9. *Fix any odd integer $k > 0$. Then as $g \to \infty$, the variety $\mathrm{Sym}^k(C)$ fails the Hasse principle for a proportion approaching 100% of locally soluble hyperelliptic curves C over $\mathbb{Q}$ of genus g.*

One may ask what is the obstruction to the Hasse principle for the varieties J^1 and $\mathrm{Sym}^k(C)$ occurring in Theorem 2 and Corollary 9, respectively. In both cases, the obstruction arises from the non-existence of a locally soluble two-cover of J^1. As shown by Skorobogatov [33, Theorem 6.1.1] (see also Stoll [34, Remark 6.5 & Theorem 7.1]), using the descent theory of Colliot-Thélène and Sansuc [14], this obstruction yields a case of the Brauer-Manin obstruction for both J^1 and $\mathrm{Sym}^k(C)$. Therefore, we obtain:

Theorem 10. *Fix any $g \geq 1$. For a positive proportion of locally soluble hyperelliptic curves C over $\mathbb{Q}$ of genus g, the variety J^1 of dimension g has a Brauer–Manin obstruction to having a rational point.*

Theorem 11. *Fix any odd integer $k > 0$. As $g \to \infty$, for a density approaching 100% of locally soluble hyperelliptic curves C over $\mathbb{Q}$ of genus g, the variety $\mathrm{Sym}^k(C)$ of dimension k has a Brauer–Manin obstruction to having a rational point.*

Recall that the index $I(C)$ of a curve $C/\mathbb{Q}$ is the least positive degree of a $\mathbb{Q}$-rational divisor D on C. Equivalently, it is the greatest common divisor of all degrees $[K:\mathbb{Q}]$ of finite field extensions $K/\mathbb{Q}$ such that C has a K-rational point. Then Theorems 1 and 2 are also equivalent to:

Theorem 12. *For any $g \geq 1$, a positive proportion of locally soluble hyperelliptic curves C of genus g over $\mathbb{Q}$ have index 2.*

We will actually prove more general versions of all of these results, where for each $g \geq 1$ we range over *any* "admissible" congruence family of hyperelliptic curves C over $\mathbb{Q}$ of genus g for which $\mathrm{Div}^1(C)$ (but not necessarily C) is locally soluble; see Definition 43 for the definition of "admissible".

We obtain Theorem 5 from Theorem 6 by combining it with a result of Dokchitser and Dokchitser (see Appendix A), which states that a positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ of genus $g \geq 1$ have even (or odd) 2-Selmer rank. Indeed, suppose that C is a locally soluble hyperelliptic curve whose 2-Selmer set $\mathrm{Sel}_2(J^1)$ is nonempty. Then the cardinality of $\mathrm{Sel}_2(J^1)$ is equal to the order of the finite elementary abelian 2-group $\mathrm{Sel}_2(J)$. As we have shown earlier, for 100% of locally soluble hyperelliptic curves, the group $\mathrm{Sel}_2(J)$ contains at least 2 elements, namely the trivial class and the class $W[2]$. Hence the cardinality of $\mathrm{Sel}_2(J^1)$ is at least 2. Moreover, if the 2-Selmer rank of the Jacobian is even, then the set $\mathrm{Sel}_2(J^1)$ (when nonempty) will have size at least 4. Therefore, Theorem 6 (and Appendix A) implies that for a positive proportion of locally soluble hyperelliptic curves, the Selmer set $\mathrm{Sel}_2(J^1)$ is empty. This proves Theorem 5.

We prove Theorem 6 by relating the problem to a purely algebraic one involving pencils of quadrics. Let A and B be two symmetric bilinear forms over $\mathbb{Q}$ in $n = 2g+2$ variables, and assume that the corresponding pencil of quadrics in $\mathbb{P}^{n-1}$ is generic. Over the complex numbers, the Fano variety $F = F(A,B)$ of common maximal isotropic subspaces of A and B is isomorphic to the Jacobian J of the hyperelliptic curve given by $C : z^2 = \mathrm{disc}(Ax - By) := (-1)^{g+1}\det(Ax - By)$ (cf. [29], [19], [16]); furthermore, all such pairs (A,B) with the same discriminant binary form are $\mathrm{SL}_n(\mathbb{C})$-equivalent.

However, as shown in [37], over $\mathbb{Q}$ the situation is much different. Given A and B, the Fano variety $F = F(A,B)$ might not have any rational points. In general, F is a principal homogeneous space for J whose class $[F]$ in $H^1(\mathbb{Q},J)$ has order dividing 4 and satisfies $2[F] = [J^1]$; hence F gives a two-cover of J^1 (see [37] or §4 for more details on the properties of the Fano variety). Moreover, given a hyperelliptic curve $C : z^2 = f(x,y)$ over $\mathbb{Q}$ of genus g (equivalently, a binary form of degree $n = 2g+2$ over $\mathbb{Q}$ with nonzero discriminant), there might not exist *any* pair (A,B) of symmetric bilinear forms over $\mathbb{Q}$ such that $f(x,y) = \mathrm{disc}(Ax - By)$! This raises the natural question: for which binary forms $f(x,y)$ of degree $n = 2g+2$ and nonzero discriminant over $\mathbb{Q}$ does there exist a pair (A,B) of symmetric bilinear forms in n variables over $\mathbb{Q}$ such that $f(x,y) = \mathrm{disc}(Ax - By)$?

In this paper, we give a geometric answer to this question in terms of the generalized Jacobian $J_{\mathfrak{m}}$ of the hyperelliptic curve $C : z^2 = f(x,y)$. Assume for simplicity that $f(x,y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$ has first coefficient $f_0 \neq 0$, so that the curve C has two distinct points P and P' above the point $\infty = (1,0)$ on $\mathbb{P}^1$. These points are rational and conjugate over the field $\mathbb{Q}(\sqrt{f_0})$. Let $\mathfrak{m} = P + P'$ be the corresponding modulus over $\mathbb{Q}$ and let $C_{\mathfrak{m}}$ denote the singular curve associated to this modulus as in [30, Ch. IV, §4]. Then $C_{\mathfrak{m}}$ is given by the equation $z^2 = f(x,y)y^2$, and has an ordinary double point at infinity. The *generalized Jacobian* of C associated to the modulus $\mathfrak{m}$, denoted by $J_{\mathfrak{m}} = J_{\mathfrak{m}}(C)$, is the connected component of the identity of $\mathrm{Pic}_{C_{\mathfrak{m}}/\mathbb{Q}}/\mathbb{Z}\cdot d$, while $J^1_{\mathfrak{m}} = J^1_{\mathfrak{m}}(C)$ denotes the nonidentity component; here d denotes the hyperelliptic class of $C_{\mathfrak{m}}$ in $\mathrm{Pic}^2_{C_{\mathfrak{m}}/\mathbb{Q}}(\mathbb{Q})$ obtained by pulling back $\mathcal{O}(1)$ from $\mathbb{P}^1$. We prove:

Theorem 13. *Let $f(x,y)$ denote a binary form of even degree $n = 2g+2$ over $\mathbb{Q}$, with nonzero discriminant and nonzero first coefficient. Then there exists a pair (A,B) of symmetric bilinear forms over $\mathbb{Q}$ in n variables satisfying $f(x,y) = \mathrm{disc}(Ax - By)$ if and only if there exists a two-cover of homogeneous spaces $F_{\mathfrak{m}} \to J^1_{\mathfrak{m}}$ for $J_{\mathfrak{m}}$ over $\mathbb{Q}$, or equivalently, if and only if the class of the homogeneous space $J^1_{\mathfrak{m}}$ is divisible by 2 in the group $H^1(\mathbb{Q}, J_{\mathfrak{m}})$.*

See Theorem 24 for a number of other equivalent conditions for the existence of A and B satisfying $f(x,y) = \mathrm{disc}(Ax - By)$. It is of significance that the singular curve $C_{\mathfrak{m}}$ and the generalized Jacobian $J_{\mathfrak{m}}$ appear in Theorem 13. The generalized Jacobians appeared in [28] for the purpose of doing 2-descent on the Jacobians of hyperelliptic curves with no rational Weierstrass point. As noted in [28, Footnote 2], in this case it is not always enough to study only unramified covers of C; one needs also covers of C unramified away from the points above some fixed point on $\mathbb{P}^1$.

The group $\mathrm{SL}_n(\mathbb{Q})$ acts on the space $\mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$ of pairs (A,B) of symmetric bilinear forms on an n-dimensional vector space, and $\mu_2 \subset \mathrm{SL}_n$ acts trivially since $n = 2g+2$ is even. The connection with Theorem 6 arises from the fact that we may parametrize elements of $\mathrm{Sel}_2(J^1)$ by certain orbits for the action of the group $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$ on the space $\mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$. We say that an element $(A,B) \in \mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$, or its $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-orbit, is *locally soluble* if the associated Fano variety $F(A,B)$ has a point locally over every place of $\mathbb{Q}$. Then we prove the following bijection:

Theorem 14. *Let $f(x,y)$ denote a binary form of even degree $n = 2g+2$ over $\mathbb{Q}$ such that the hyperelliptic curve $C : z^2 = f(x,y)$ is locally soluble. Then the $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-orbits of locally soluble pairs (A,B) of symmetric bilinear forms in n variables over $\mathbb{Q}$ such that $f(x,y) = \mathrm{disc}(Ax - By)$ are in bijection with the elements of the 2-Selmer set $\mathrm{Sel}_2(J^1)$.*

To obtain Theorem 6, we require a version of Theorem 14 for integral orbits. Let $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ denote the space of pairs (A,B) of $n \times n$ symmetric bilinear forms over $\mathbb{Z}$. Then we prove the following theorem on integral representatives:

Theorem 15. *There exists a positive integer κ depending only on n such that, for any integral binary form $f(x,y)$ of even degree $n = 2g+2$ with $C : z^2 = f(x,y)$ locally soluble over $\mathbb{Q}$, every $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-orbit of locally soluble pairs $(A,B) \in \mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$ such that $\mathrm{disc}(Ax - By) = \kappa^2 f(x,y)$ contains an element in $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$. In other words, the $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-equivalence classes of locally soluble pairs $(A,B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ such that $\mathrm{disc}(Ax - By) = \kappa^2 f(x,y)$ are in bijection with the elements of $\mathrm{Sel}_2(J^1)$.*

We will prove Theorem 15 for $\kappa = 4$ but we expect this can be improved. We use Theorem 15, together with the results of [1] giving the number of $\mathrm{SL}_n(\mathbb{Z})$-orbits on $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ having bounded height, and a sieve, to deduce Theorem 6.

We note that the emptiness of $J^1(\mathbb{Q})$ for hyperelliptic curves C over $\mathbb{Q}$ has been demonstrated previously for certain special algebraic families. In [13], Colliot-Thélène and Poonen constructed one-parameter algebraic families of curves $C = C_t$ of genus 1 and genus 2 for which the varieties J^1 have a Brauer-Manin obstruction to having a rational point for all $t \in \mathbb{Q}$. (We note that the family of genus 2 curves considered in [13] consists of hyperelliptic curves C over $\mathbb{Q}$ with locally soluble $J^1(C)$ but not locally soluble $\mathrm{Div}^1(C)$.) For arbitrary genus $g \geq 6$ with $4 \nmid g$, Dong Quan [20] constructed such one-parameter algebraic families of locally soluble hyperelliptic curves $C = C_t$ having empty $J^1(\mathbb{Q})$ for every $t \in \mathbb{Q}$.

This paper is organized as follows. In Section 2, we introduce the key representation $2 \otimes \mathrm{Sym}_2(n)$ of SL_n on pairs of symmetric bilinear forms that we will use to study the arithmetic of

hyperelliptic curves. We adapt the results of Wood [40] to study the orbits of this representation over a general Dedekind domain D whose characteristic is not equal to 2. In Section 3, we introduce hyperelliptic curves and some of the relevant properties of their generalized Jacobians. In Section 4, we then relate hyperelliptic curves to generic pencils of quadrics over a field K of characteristic not equal to 2, and we review the results that we will need from [37]. In Section 5, we then study *regular* pencils of quadrics, which allows us to determine which binary n-ic forms over K arise as the discriminant of a pencil of quadrics over K; in particular, we prove Theorem 13.

In Section 6, we describe how the K-*soluble* orbits (i.e., orbits of those (A, B) over K such that $F(A, B)$ has a K-rational point), having associated hyperelliptic curve C over K, are parametrized by elements of the set $J^1(K)/2J(K)$. We study the orbits over some arithmetic fields in more detail in Section 7 and then we focus on global fields and discuss *locally soluble* orbits in Section 8. We show that the locally soluble orbits over $\mathbb{Q}$, having associated hyperelliptic curve C over $\mathbb{Q}$ are parametrized by the elements of the finite set $\mathrm{Sel}_2(J^1)$, proving Theorem 14. The existence of integral orbits (Theorem 15) is demonstrated in Section 9. We then discuss the counting results from [1] that we need in Section 10, and discuss the details of the required sieve in Section 11. Finally, we complete the proofs of Theorems 6 and 7 in the final Section 12.

2 Orbits of pairs of symmetric bilinear forms over a Dedekind domain

In this section, we study the orbits of our key representation $2 \otimes \mathrm{Sym}_2(n)$ over a Dedekind domain D. In later sections, we will specialize to the case when D is a field, $\mathbb{Z}_p$ or $\mathbb{Z}$. We will also relate these results on orbits to the arithmetic of hyperelliptic curves.

Let K denote the quotient field of D. We assume throughout this paper that the characteristic of K is not equal to 2. Let $n \geq 2$ be an integer. The group $\mathrm{SL}_n(D)$ acts on the D-module of pairs (A, B) of symmetric bilinear forms on a free D-module W of rank n. After a choice of basis for W, this is the representation $D^2 \otimes \mathrm{Sym}_2 D^n = \mathrm{Sym}_2 D^n \oplus \mathrm{Sym}_2 D^n$.

The coefficients of the binary n-ic form

$$f(x, y) = \mathrm{disc}(xA - yB) := (-1)^{n(n-1)/2} \det(xA - yB) = f_0 x^n + f_1 x^{n-1} y + \cdots + f_n y^n,$$

which we call the *invariant binary n-ic form* of the element $(A, B) \in D^2 \otimes \mathrm{Sym}_2 D^n$, give $n + 1$ polynomial invariants of degree n which freely generate the ring of polynomial invariants over D. We also have the invariant *discriminant* polynomial $\Delta(f) = \Delta(f_0, f_1, \ldots, f_n)$ given by the discriminant of the binary form f, which has degree $2n(n - 1)$ in the entries of A and B.

In Wood's work [40], the orbits of $\mathrm{SL}_n^{\pm}(T) = \{g \in \mathrm{GL}_n(T) : \det(g) = \pm 1\}$ on $T^2 \otimes \mathrm{Sym}_2 T^n$ were classified for general rings (and in fact even for general base schemes) T in terms of ideal classes of rings of rank n over T. In this section, we translate these results into a form that we will use later on, in the important special case where $T = D$ is a Dedekind domain with quotient field K. In particular, we will need to use the actions by the groups $\mathrm{SL}_n(D)$ and in the case n is even, the group $(\mathrm{SL}_n / \mu_2)(D)$ rather than $\mathrm{SL}_n^{\pm}(D)$. This causes some key changes in the parametrization data and will indeed be important for us when we make the connection with hyperelliptic curves.

Let us assume that $f_0 \neq 0$ and write $f(x, 1) = f_0 g(x)$, where $g(x)$ has coefficients in the quotient field K and has n distinct roots in a separable closure K^s of K. Let $L = L_f := K[x]/g(x)$ be the corresponding étale algebra of rank n over K, and let θ be the image of x in the algebra L. Then

$g(\theta) = 0$ in L. Let $g'(x)$ be the derivative of $g(x)$ in $K[x]$; since $g(x)$ is separable, the value $g'(\theta)$ must be an invertible element of L. We define $f'(\theta) = f_0 g'(\theta)$ in $L^\times$.

For $k = 1, 2, \ldots, n-1$, define the integral elements

$$\zeta_k = f_0\theta^k + f_1\theta^{k-1} + \cdots + f_{k-1}\theta$$

in L, and let $R = R_f$ be the free D-submodule of L having D-basis $\{1, \zeta_1, \zeta_2, \ldots, \zeta_{n-1}\}$. For $k = 0, 1, \ldots, n-1$, let $I(k)$ be the free D-submodule of L with basis $\{1, \theta, \theta^2, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\}$. Then $I(k) = I(1)^k$, and $I(0) = R \subset I(1) \subset \cdots \subset I(n-1)$. Note that $I(n-1)$ has the power basis $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, but that the elements of $I(n-1)$ need not be integral when f_0 is not a unit in D.

A remarkable fact (cf. [9], [25, Proposition 1.1], [39, §2.1]) is that R is a D-order in L of discriminant $\Delta(f)$, and the free D-modules $I(k)$ are all fractional ideals of R. The fractional ideal $(1/f'(\theta))I(n-2)$ is the dual of R under the trace pairing on L, and the fractional ideal $I(n-3)$ will play a crucial role in the parametrization of orbits in our representation.

We then have the following translation of [40, Theorem 1.3] in the case of the action of $\mathrm{SL}_n(D)$ on $D^2 \otimes \mathrm{Sym}_2 D^n$, where D is a Dedekind domain:

Theorem 16. *Assume that $f(x, y)$ is a binary form of degree n over D with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection (to be described below) between orbits for $\mathrm{SL}_n(D)$ on $D^2 \otimes \mathrm{Sym}_2 D^n$ with invariant form f and equivalence classes of triples (I, α, s), where I is a fractional ideal for R, $\alpha \in L^\times$, and $s \in K^\times$, satisfying the relations $I^2 \subset \alpha I(n-3)$, $N(I)$ is the principal fractional ideal sD in K, and $N(\alpha) = s^2 f_0^{n-3}$ in $K^\times$. The triple (I, α, s) is equivalent to the triple $(cI, c^2\alpha, N(c)s)$ for any $c \in L^\times$. The stabilizer of a triple (I, α, s) is $S^\times[2]_{N=1}$ where $S = \mathrm{End}_R(I) \subset L$.*

From a triple (I, α, s), we construct an orbit as follows. Since $N(I)$ is the principal D-ideal sD, the projective D-module I of rank n is free. Since $I^2 \subset \alpha I(n-3)$, we obtain two symmetric bilinear forms on the free module I by defining $\langle \lambda, \mu \rangle_A$ and $\langle \lambda, \mu \rangle_B$ as the respective coefficients of ζ_{n-1} and ζ_{n-2} in the basis expansion of the product $\lambda\mu/\alpha$ in $I(n-3)$. We obtain an $\mathrm{SL}_n(D)$-orbit of two symmetric $n \times n$ matrices (A, B) over D by taking the Gram matrices of these forms with respect to any ordered basis of I that gives rise to the basis element $s(1 \wedge \zeta_1 \wedge \zeta_2 \wedge \ldots \wedge \zeta_{n-1})$ of the top exterior power of I over D. This normalization deals with the difference between $\mathrm{SL}_n(D)$- and $\mathrm{GL}_n(D)$-orbits. The stabilizer statement follows because elements in $S^\times[2]_{N=1}$ are precisely the elements of $L^\times_{N=1}$ that preserve the map $\frac{1}{\alpha}\times : I \times I \to I(n-3)$.

Conversely, given an element $(A, B) \in D^2 \otimes \mathrm{Sym}_2 D^n$, we construct the ring $R = R_f$ from f as described above, where $f(x, y) = \mathrm{disc}(xA - yB)$. The R-module I is then constructed by letting $\theta \in L$ act on K^n by the matrix $A^{-1}B$. Then $\zeta_1 = f_0\theta \in R$ preserves the lattice D^n. Similarly, formulas for the action of each $\zeta_i \in R$ on D^n, in terms of integral polynomials in the entries of A and B, can be worked out when A is assumed to be invertible; these same formulas can then be used to show that D^n is an R-module, even when A is not invertible. See [40, §3.1] for the details.

When $n = 2m$ is even, the larger group $(\mathrm{SL}_n/\mu_2)(D)$ acts on the representation $D^2 \otimes \mathrm{Sym}_2 D^n$, and distinct orbits for the subgroup $\mathrm{SL}_n(D)/\mu_2(D)$ may become identified as a single orbit for the larger group. Since a projective module of rank n over D whose top exterior power is a free module is itself free of rank n by [24, Theorem 1.6], we have $H^1(D, \mathrm{SL}_n) = 1$ and hence an exact sequence of groups

$$1 \to \mathrm{SL}_n(D)/\mu_2(D) \to (\mathrm{SL}_n/\mu_2)(D) \to H^1(D, \mu_2) \to 1.$$

By Kummer theory, the quotient group $H^1(D,\mu_2)$ lies in an exact sequence

$$1 \to D^\times/D^{\times 2} \to H^1(D,\mu_2) \to \mathrm{Pic}(D)[2] \to 1.$$

The image of the group $H^1(D,\mu_2)$ in $H^1(K,\mu_2) = K^\times/K^{\times 2}$ is the subgroup $K^{\times(2)}/K^{\times 2}$ of elements t such that the principal ideal $tD = M^2$ is a square, and the map to $\mathrm{Pic}(D)[2]$ is given by mapping such an element t to the class of M. The action of t on a triple (I,α,s) with invariant form f is given by

$$t\cdot(I,\alpha,s) = (MI, t\alpha, t^{n/2}s).$$

Along with the action of $\mathrm{SL}_n(D)$ on such triples, this gives an action of $(\mathrm{SL}_n/\mu_2)(D)$ on these triples. The equivalence classes of triples under this action of $(\mathrm{SL}_n/\mu_2)(D)$ give the orbits of $(\mathrm{SL}_n/\mu_2)(D)$ with invariant form f. The stabilizer of the triple (I,α,s) contains the finite group $S^\times[2]_{N=1}/D^\times[2]$ where $S = \mathrm{End}_R(I) \subset L$, since that is the image of the stabilizer from $\mathrm{SL}_n(D)$.

Theorem 17. *Assume that $f(x,y)$ is a binary form of even degree n over D with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection between orbits for $(\mathrm{SL}_n/\mu_2)(D)$ on $D^2 \otimes \mathrm{Sym}_2 D^n$ with invariant form f and equivalence classes of triples (I,α,s), where I is a fractional ideal for R, $\alpha \in L^\times$, and $s \in K^\times$, satisfying the relations $I^2 \subset \alpha I(n-3)$, $N(I)$ is the principal fractional ideal sD in K, and $N(\alpha) = s^2 f_0^{n-3}$ in $K^\times$. The triple (I,α,s) is equivalent to the triple $(cMI, c^2t\alpha, N(c)t^{n/2}s)$ for any $c \in L^\times$ and $t \in K^{\times(2)}$, where $tD = M^2$. The stabilizer of the triple (I,α,s) is an elementary abelian 2-group which contains $S^\times[2]_{N=1}/D^\times[2]$ where $S = \mathrm{End}_R(I) \subset L$.*

Remark 18. We can simplify the statement of Theorem 17 when the domain D is a principal ideal domain and every fractional ideal for the D-order R is principal. In that case, the fractional ideal I of R is completely determined by the pair (α,s) and the identities $I^2 \subset (\alpha)I(n-3)$, $N(I) = (s)$, and $N(\alpha) = s^2 f_0^{n-3}$. Indeed, together these force $I^2 = (\alpha)I(n-3)$. There is a bijection from the set of equivalence classes of α to the set $(R^\times/R^{\times 2}D^\times)_{N=f_0}$. Moreover, we have $S = \mathrm{End}_R(I) = R$ and $K^{\times(2)} = D^\times K^{\times 2}$. An element $t \in K^{\times(2)}/K^\times$ preserves an $\mathrm{SL}_n(D)$-orbit if and only if $t = c^2 \in R^{\times 2}$ for some $c \in R^\times$ with $N(c) = t^{n/2}$. Note if $t = c^2$, then $N(c) = (-t)^{n/2}$. Hence the stabilizer in $(\mathrm{SL}_n/\mu_2)(D)$ of a triple (I,α,s) equals $(R^\times[2])_{N=1}/D^\times[2]$ if $n \equiv 2 \pmod 4$ and fits into the exact sequence

$$1 \to (R^\times[2])_{N=1}/D^\times[2] \to \mathrm{Stab}_{(\mathrm{SL}_n/\mu_2)(D)}(I,\alpha,s) \to (R^{\times 2}\cap D^\times)/D^{\times 2} \to 1, \tag{3}$$

when $n \equiv 0 \pmod 4$. When L is not an algebra over a quadratic extension of K, the quotient $(R^{\times 2}\cap D^\times)/D^{\times 2}$ is trivial.

In particular, when $D = K$ is a field, we recover [6, Theorems 7 and 8]. These versions of Theorems 16 and 17 over a field K will also be important in the sequel. For convenience, we restate them below.

Corollary 19. *Assume that $f(x,y)$ is a binary form of degree n over K with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection between orbits for $\mathrm{SL}_n(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant form f and equivalence classes of pairs (α,s), where $\alpha \in L^\times$ and $s \in K^\times$, satisfying $N(\alpha) = s^2 f_0^{n-3}$ in $K^\times$. The pair (α,s) is equivalent to the pair $(c^2\alpha, N(c)s)$ for any $c \in L^\times$. The stabilizer of the orbit corresponding to a pair (α,s) is the finite commutative group scheme $(\mathrm{Res}_{L/K}\mu_2)_{N=1}$ over K.*

It follows from Corollary 19 that the set of $\mathrm{SL}_n(K)$-orbits is either in bijection with or has a 2-to-1 map to $(L^\times/L^{\times 2})_{N=f_0}$, in accordance with whether $f(x,y)$ has an odd degree factor over K or not, respectively. Indeed, the pair (α, s) is equivalent to the pair $(\alpha, -s)$ if and only if there is an element $c \in L^\times$ with $c^2 = 1$ and $N(c) = -1$. The stabilizers correspond to the K-rational even degree factors of $f(x,y)$.

Corollary 20. *Assume that $f(x,y)$ is a binary form of even degree n over K with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection between orbits of $(\mathrm{SL}_n/\mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant form f and equivalence classes of pairs (α, s) where $\alpha \in L^\times$ and $s \in K^\times$ satisfying $N(\alpha) = s^2 f_0^{n-3}$ in $K^\times$. The pair (α, s) is equivalent to the pair $(c^2 t\alpha, N(c)t^{n/2}s)$ for any $c \in L^\times$ and $t \in K^{\times(2)} = K^\times$. The stabilizer of the orbit corresponding to a pair (α, s) is the finite commutative group scheme $(\mathrm{Res}_{L/K}\,\mu_2)_{N=1}/\mu_2$ over K.*

It follows from Corollary 20 that the set of $(\mathrm{SL}_n/\mu_2)(K)$-orbits is either in bijection with or has a 2-to-1 map to $(L^\times/(L^{\times 2}K^\times))_{N=f_0}$, in accordance with whether $f(x,y)$ has an odd factorization over K or not, respectively. Here an *odd factorization* of $f(x,y)$ over K is a factorization of the form $f(x,y) = g(x,y)h(x,y)$, where g and h are odd degree binary forms that are either K-rational or are conjugate over some quadratic extension of K. Meanwhile, the elements of the stabilizer correspond to even factorizations of $f(x,y)$. When n is congruent to 2 modulo 4, an even factorization of $f(x,y)$ must be of the form $g(x,y)h(x,y)$ where both g and h are K-rational even degree binary forms. In other words, they already appear in the stabilizers in $\mathrm{SL}_n(K)$. When n is congruent to 0 modulo 4, $f(x,y)$ can have even factorizations into conjugate binary forms over some quadratic extensions K'/K. The image of a stabilizer element corresponding to such a factorization in $(L^{\times 2} \cap K^\times)/K^{\times 2}$ is the class corresponding to the quadratic extension K'.

3 Hyperelliptic curves, divisor classes, and generalized Jacobians

Assume from now on that $n \geq 2$ is even and write $n = 2g + 2$. Fix a field K of characteristic not 2. In order to interpret the orbits for $\mathrm{SL}_n(K)$ and $(\mathrm{SL}_n/\mu_2)(K)$ having a fixed invariant binary form, we first review some of the arithmetic and geometry of hyperelliptic curves of genus g over K. As in [21], we define a hyperelliptic curve over K as a smooth, projective curve over K with a 2-to-1 map to the projective line over K, although we now treat the general case (without assuming any fixed K-rational points at infinity.)

Let $f(x,y) = f_0x^{2g+2} + f_1x^{2g+1}y + \cdots + f_{2g+2}y^{2g+2}$ be a binary form of degree $2g+2$ over K, with $\Delta \neq 0$ and $f_0 \neq 0$. We associate to $f(x,y)$ the hyperelliptic curve C over K with equation

$$z^2 = f(x,y).$$

This defines a smooth curve of genus g, as a hypersurface of degree $2g+2$ in the weighted projective plane $\mathbb{P}(1,1,g+1)$. The weighted projective plane embeds as a surface in $\mathbb{P}^{g+2}$ via the map $(x,y,z) \to (x^{g+1}, x^g y, \ldots, y^{g+1}, z)$. The image is a cone over the rational normal curve in $\mathbb{P}^{g+1}$, which has a singularity at the vertex $(0,0,\ldots,1)$ when $g \geq 1$. The curve C is the intersection of this surface with a quadric hypersurface that does not pass through the vertex of the cone. Finally, the linear series on C of projective dimension $g+2$ and degree $2g+2$ that gives this embedding is the sum of the all the Weierstrass points (i.e., points with $z = 0$).

There are two points $P = (1, 0, z_0)$ and $P' = (1, 0, -z_0)$ at infinity, where $z_0^2 = f_0$. If f_0 is a square in $K^\times$, then these points are rational over K. If not, then they are rational over the quadratic extension $K' = K(\sqrt{f_0})$. Let w be the rational function z/y^{g+1} on C, and let t be the rational function x/y on C. Both are regular outside of the two points P and P' with $y = 0$, where they have poles of order $g + 1$ and 1 respectively. The field of rational functions on C is given by $K(C) = K(t, w)$, with $w^2 = f(t, 1) = f_0 t^{2g+2} + f_1 t^{2g+1} + \cdots + f_{2g+2}$, and the subring of functions that are regular outside of P and P' is $K[t, w] = K[t, \sqrt{f(t, 1)}]$ [21].

Let $\mathfrak{m}$ be the modulus $\mathfrak{m} = P + P'$ on C and let $C_\mathfrak{m}$ be the singular curve constructed from C and this modulus in [30, Ch. IV, no. 4]. Then $C_\mathfrak{m}$ has equation

$$z^2 = f(x, y)y^2$$

of degree $2g + 4$ in $\mathbb{P}(1, 1, g + 2)$. This defines a singular, projective curve of arithmetic genus $g + 1$ whose normalization is C. There is now a single point $Q = (1, 0, 0)$ at infinity, which is an ordinary double point whose tangents are rational over the quadratic extension field K'.

Let $\mathrm{Pic}_{C/K}$ and $\mathrm{Pic}_{C_\mathfrak{m}/K}$ denote the Picard functors of the projective curves C and $C_\mathfrak{m}$ respectively. These are represented by commutative group schemes over K, whose component groups are both isomorphic to $\mathbb{Z}$. Let K^s be a fixed separable closure of K and let E be any extension of K contained in K^s. The E-rational points of $\mathrm{Pic}_{C/K}$ correspond bijectively to the divisor classes on C over the separable closure K^s that are fixed by the Galois group $\mathrm{Gal}(K^s/E)$. When the curve C has no E-rational points, an E-rational divisor class on C may not be represented by an E-rational divisor. The subgroup of classes in $\mathrm{Pic}_{C/K}(E)$ that are represented by E-rational divisors is just the image of $\mathrm{Pic}(C/E) = H^1(C/E, \mathbb{G}_m)$ in $H^0(E, H^1(C/K^s, \mathbb{G}_m))$, under the map induced by the spectral sequence for the morphism $C/E \to \mathrm{Spec}\, E$. From this spectral sequence, we also obtain an injection from the quotient group to the Brauer group of K (cf. [33, §2.3], [10, Ch. 8]):

$$\mathrm{Pic}_{C/K}(K)/\mathrm{Pic}(C/K) \to H^2(K, \mathbb{G}_m) = \mathrm{Br}(K).$$

Since C has a rational point over the quadratic extension $K' = K(\sqrt{f_0})$, the image of this injection is contained in the subgroup $\mathrm{Br}(K'/K) = K^\times/N(K'^\times)$. Every class in $\mathrm{Br}(K'/K)$ corresponds to a quaternion algebra D over K that is split by K', or equivalently, to a curve of genus zero over K with two conjugate points rational over K'.

Proposition 21. *If a hyperelliptic curve C over K has a rational divisor of odd degree, or equivalently a rational point over an extension of K of odd degree, then every K-rational divisor class is represented by a K-rational divisor. If K is a global field and $\mathrm{Div}^1(C)$ is locally soluble, then every K-rational divisor class is represented by a K-rational divisor.*

Indeed, a quaternion algebra split by an odd degree extension of K is already split over K. Similarly, a quaternion algebra over a global field that splits locally everywhere is split globally.

The distinction between K-rational divisor classes and K-rational divisors does not arise for the curve $C_\mathfrak{m}$, which always have the K-rational singular point Q. Hence the points of $\mathrm{Pic}_{C_\mathfrak{m}/K}$ over E correspond to the classes of divisors that are rational over E and are prime to $\mathfrak{m}$, modulo the divisors of functions with $f \equiv 1$ modulo $\mathfrak{m}$. We have an exact sequence of smooth group schemes over K :

$$0 \to T \to \mathrm{Pic}_{C_\mathfrak{m}/K} \to \mathrm{Pic}_{C/K} \to 0, \tag{4}$$

where T is the one-dimensional torus that is split by K'. Taking the long exact sequence in Galois cohomology, and noting that the image of $\mathrm{Pic}_{C_\mathfrak{m}/K}(K)$ in $\mathrm{Pic}_{C/K}(K)$ is precisely the subgroup $\mathrm{Pic}(C/K) = H^1(C/K, \mathbb{G}_m)$ represented by K-rational divisors, we recover the injection

$$\mathrm{Pic}_{C/K}(K)/\mathrm{Pic}(C/K) \to H^1(K,T) = K^\times/N(K'^\times) = \mathrm{Br}(K'/K).$$

To see this geometrically, note that the fiber over a K-rational point P of $\mathrm{Pic}_{C/K}$ is a principal homogeneous space for T over K, which is a curve of genus zero with two conjugate points over K' removed. This curve of genus zero determines the image of P in $\mathrm{Br}(K'/K)$.

The connected components of the identity of the Picard schemes $J = \mathrm{Pic}^0_{C/K}$ and $J_\mathfrak{m} = \mathrm{Pic}^0_{C_\mathfrak{m}/K}$ are the Jacobian and generalized Jacobian of [30, Ch. V]. They correspond to the divisor classes of degree zero on these curves. The exact sequence in (4) restricts to the following exact sequence [30, Ch. V, §3]:

$$0 \to T \to J_\mathfrak{m} \to J \to 0. \tag{5}$$

There is a line bundle of degree 2 on $C_\mathfrak{m}$ (and hence on C) which is the pull-back of the line bundle $\mathcal{O}(1)$ from the projective line under the map $(x,y,z) \to (x,y)$. This is represented by the K-rational divisor $d = (R) + (R')$ prime to $\mathfrak{m}$ consisting of the two points above a point (x_0, y_0) on the projective line, whenever y_0 is nonzero. The quotient groups $\mathrm{Pic}_{C/K}/\mathbb{Z}\cdot d = J \sqcup J^1$ and $\mathrm{Pic}_{C_\mathfrak{m}/K}/\mathbb{Z}\cdot d = J_\mathfrak{m} \sqcup J^1_\mathfrak{m}$ both have two connected components, represented by the divisor classes of degree 0 and 1. There are morphisms

$$\begin{aligned} C &\longrightarrow J^1 \\ C - \{P, P'\} &\longrightarrow J^1_\mathfrak{m} \end{aligned}$$

defined over K, which take a point to the corresponding divisor class of degree 1 [30, Ch V, §4].

Proposition 22. *Let $f(x,y) = f_0x^{2g+2} + f_1x^{2g+1}y + \cdots + f_{2g+2}y^{2g+2}$ be a binary form with nonzero discriminant and nonzero f_0. Let $C : z^2 = f(x,y)$ and $C_\mathfrak{m} : z^2 = f(x,y)y^2$ denote the associated hyperelliptic curve and singular curve with Jacobian J and generalized Jacobian $J_\mathfrak{m}$. Let $L = K[x]/f(x,1)$ denote the corresponding étale algebra of rank $2g+2$. Then:*

1. *The 2-torsion subgroup $J_\mathfrak{m}[2]$ of $J_\mathfrak{m}$ is isomorphic to the group scheme $(\mathrm{Res}_{L/K}\mu_2)_{N=1}$. Its K-rational points correspond to the even degree factors of $f(x,y)$ over K.*

2. *The 2-torsion subgroup $J[2]$ of J is isomorphic to the group scheme $(\mathrm{Res}_{L/K}\mu_2)_{N=1}/\mu_2$. Its K-rational points correspond to the even factorizations of $f(x,y)$ over K.*

3. *The 2-torsion $W_\mathfrak{m}[2]$ in the component $J^1_\mathfrak{m}$ of $\mathrm{Pic}_{C_\mathfrak{m}/K}/\mathbb{Z}\cdot d = J_\mathfrak{m} \sqcup J^1_\mathfrak{m}$, is a torsor for $J_\mathfrak{m}[2]$ whose K-rational points correspond to the odd degree factors of $f(x,y)$ over K.*

4. *The 2-torsion $W[2]$ in the component J^1 of $\mathrm{Pic}_{C/K}/\mathbb{Z}\cdot d = J \sqcup J^1$ is a torsor for $J[2]$ whose K-rational points correspond to the odd factorizations of $f(x,y)$ over K.*

Here an odd (resp. even) factorization of $f(x,y)$ over K is a factorization of the form $f = gh$, where g and h are odd (resp. even) degree binary forms that are either defined over K or are conjugate over some quadratic extension of K. Note that giving a factor of $f(x,y)$ is the same as giving a subset of Weierstrass points—hence the choice of the letter "W" in $W[2]$ and $W_\mathfrak{m}[2]$.

Proof. To prove the proposition, we observe that the 2-torsion points of $J_{\mathfrak{m}}$ over the separable closure K^s are represented by the classes of divisors of the form $(P_1) + (P_2) + \cdots + (P_{2m}) - md$, where each $P_i = (x_i, 1, 0)$ comes from a distinct root x_i of $f(x, 1)$ [22, §4]. Hence the points of $J_{\mathfrak{m}}[2]$ over K^s correspond bijectively to the factors of even degree of $f(x, y)$ over K^s. Since the Galois group acts by permutation of the roots, we have a canonical isomorphism $J_{\mathfrak{m}}[2] \simeq (\mathrm{Res}_{L/K}\mu_2)_{N=1}$. On the quotient J, there is a single relation: $(P_1) + (P_2) + \cdots + (P_{2g+2}) - (g+1)d = \mathrm{div}(y) \equiv 0$, so $J[2] \simeq (\mathrm{Res}_{L/K}\mu_2)_{N=1}/\mu_2$. The last two statements of Proposition 22 follow similarly. □

Finally, we note that the Weil pairing $J[2] \times J[2] \to \mu_2$ gives the self-duality of the finite group scheme $(\mathrm{Res}_{L/K}\mu_2)_{N=1}/\mu_2$, and the connecting homomorphism $H^1(K, J[2]) \to H^2(K, \mu_2)$ whose kernel is the image of $H^1(K, J_{\mathfrak{m}}[2])$ is cup product with the class of $W[2]$ (see [28, Proposition 10.3]).

4 Generic pencils of quadrics

In this section, we relate hyperelliptic curves to pencils of quadrics. In particular, we will see how pencils of quadrics yield two-covers of J^1 for certain hyperelliptic curves.

Let $W = K^n$ be a vector space of dimension $n \geq 3$ over K and let A and B be two symmetric bilinear forms on W. Let Q_A and Q_B be the corresponding quadric hypersurfaces in $\mathbb{P}(W)$, so Q_A is defined by the equation $\langle w, w\rangle_A = 0$ and Q_B is defined by the equation $\langle w, w\rangle_B = 0$. Let Y be the base locus of the pencil spanned by A and B, which is defined by the equations $\langle w, w\rangle_A = \langle w, w\rangle_B = 0$ in $\mathbb{P}(W)$. Then Y has dimension $n-3$ and is a smooth complete intersection if and only if the discriminant of the pencil $\mathrm{disc}(xA - yB) = f(x, y)$ has $\Delta(f) \neq 0$. In this case we say that the pencil spanned by A and B is *generic*. In this section, we will only consider generic pencils. The Fano scheme $F = F(A, B)$ is the Hilbert scheme of maximal linear subspaces of $\mathbb{P}(W)$ that are contained in Y.

When $n = 2g+1$ is odd, the Fano scheme has dimension zero and is a principal homogeneous space for the finite group scheme $\mathrm{Res}_{L/K}\mu_2/\mu_2 \simeq (\mathrm{Res}_{L/K}\mu_2)_{N=1}$. Here L is the étale algebra of rank $2g+1$ determined by the binary form $f(x, y)$. The 2^{2g} points of F over the separable closure of K correspond to the subspaces Z of W of dimension g that are isotropic for all the quadrics in the pencil, and the scheme F depends only on the $\mathrm{SL}_n(K)$-orbit of the pair (A, B).

When $n = 2g+2$ is even, the Fano scheme F is smooth and geometrically connected of dimension g, and is a principal homogeneous space for the Jacobian J of the smooth hyperelliptic curve C with equation $z^2 = f(x, y)$. A point of F corresponds to a subspace Z of W of dimension g that is isotropic for all of the quadrics in the pencil, whereas a point of C corresponds to a quadric in the pencil plus a choice of one of the two rulings of that quadric. This interpretation can be used to define a morphism $C \times F \to F$ over K, which in turn gives a simply transitive action of J on F. In this case, the Fano variety F depends only on the $(\mathrm{SL}_n/\mu_2)(K)$-orbit of the pair (A, B). Proofs of all assertions on the Fano scheme can be found in [37].

Theorem 23. ([37, Theorem 2.7]) *Let F be the Fano variety of maximal linear subspaces contained in the base locus of a generic pencil of quadrics generated by symmetric bilinear forms $(A, B) \in K^2 \otimes \mathrm{Sym}_2 K^n$. Let $f(x, y)$ denote the invariant binary form of (A, B). Let $C : z^2 = f(x, y)$ denote the corresponding hyperelliptic curve with Jacobian J. Then the disconnected variety*

$$X := J \sqcup F \sqcup J^1 \sqcup F \tag{6}$$

has a commutative algebraic group structure over K. In particular, $[F]$ as a class in $H^1(K, J)$ is 4-torsion and $2[F] = [J^1]$.

The group X contains the subgroup $\mathrm{Pic}_{C/K}\,/\mathbb{Z}\cdot d = J \sqcup J^1$ with index two. Let $F[4]$ be the principal homogeneous space for $J[4]$ consisting of the points of F of (minimal) order 4 in the group X. Multiplication by 2 in X gives finite étale covers

$$F \to J^1$$

$$F[4] \to W[2]$$

of degree 2^{2g} with an action of the group scheme $J[2]$. This shows that the class $[F]$ of the principal homogeneous space F satisfies $2[F] = [J^1]$ in the group $H^1(K, J)$. Similarly, the class of $W[2]$ in $H^1(K, J[2])$ is the image of the class $F[4]$ in $H^1(K, J[4])$ under the map $m_2 : H^1(K, J[4]) \to H^1(K, J[2])$ induced by the multiplication by 2 map from $J[4]$ to $J[2]$. In general, if an element $[F'] \in H^1(K, J[2])$ is in the image of m_2, we say $[F']$ is divisible by 2 in $H^1(K, J[4])$.

Consequently, a necessary condition on the existence of a pencil (A, B) over K with discriminant curve C is that the class of J^1 and the class of $W[2]$ should be divisible by 2 in $H^1(K, J)$ and $H^1(K, J[4])$ respectively. However, this condition is not sufficient. Consider the curve C of genus zero with equation $z^2 = -x^2 - y^2$ over $\mathbb{R}$. In this case, both J and $J[2]$ reduce to a single point, so any homogeneous space for J or $J[2]$ is trivial, and hence divisible by 2. On the other hand, since $L = \mathbb{C}$ and $f_0 = -1$ is not a norm, by Corollary 19 (or 20) there are no pencils over $\mathbb{R}$ with discriminant $f(x, y) = -x^2 - y^2$. To obtain a geometric condition that is both necessary and sufficient for the existence of a pencil, we will have to consider non-generic pencils whose invariant binary form defines the singular curve $C_{\mathfrak{m}}$. This is the object of the next section.

5 Regular pencils of quadrics

In this section, we give a list of equivalent conditions for the existence of a pencil over K whose discriminant is some given binary form $f(x, y)$. In particular, we prove Theorem 13.

Let (A, B) generate a generic pencil of bilinear forms on a vector space W of even dimension $n = 2g + 2$ over K, and let $f(x, y) = \mathrm{disc}(xA - yB)$ be its invariant binary form of degree $2g + 2$ and discriminant $\Delta(f) \neq 0$. We continue to assume that $f_0 = \mathrm{disc}(A)$ is also nonzero in K. Let (A', B') be a pair of bilinear forms on the vector space $W' = W \oplus K^2$ of dimension $n + 2 = 2g + 4$, where A' is the direct sum of A and the rank one form $\langle (a, b), (a', b') \rangle = aa'$ on K^2 and B' is the direct sum of B and the split form $\langle (a, b), (a', b') \rangle = ab' + a'b$ of rank 2. The invariant binary form of this pencil

$$\mathrm{disc}(xA' - yB') = f(x, y)y^2$$

then has a double zero at $(x, y) = (1, 0)$, and the pencil is not generic. The base locus defined by the equations $Q_{A'} = Q_{B'} = 0$ in $\mathbb{P}(W \oplus K^2)$ has an ordinary double point at the unique singular point $R = (0_W; 0, 1)$ of the quadric $Q_{A'}$. There are exactly $2g + 3$ singular quadrics in the pencil and all of them are simple cones. The K-algebra L' associated to the pencil is not étale, but is isomorphic to $L \oplus K[y]/y^2$. Even though L' is not étale, the vector space W' is a free L'-module of rank 1, so the pencil is regular in the sense of [37, §3]. Since the norms from $K[y]/y^2$ to K are precisely the squares in K, we have an equality of quotient groups $K^\times/(K^{\times 2}N(L^\times)) = K^\times/(K^{\times 2}N(L'^\times))$.

The Fano scheme $F_{\mathfrak{m}}$ of this pencil consists of the subspaces Z of dimension $g + 1$ in $W \oplus K^2$ that are isotropic for all of the quadrics in the pencil and do not contain the unique line that is the radical of the form A' (so the projective space $\mathbb{P}(Z)$, which is contained in the base locus, does not

meet the unique double point R). The Fano scheme is a smooth variety of dimension $g+1$. However, in this case $F_{\mathfrak{m}}$ is not projective. It is a principal homogeneous space for the generalized Jacobian $J_{\mathfrak{m}}$ associated to the singular curve $C_{\mathfrak{m}}$ of arithmetic genus $g+1$ and equation $z^2 = f(x,y)y^2$ in weighted projective space.

For example, when $g = 0$, the curve C is the non-singular quadric $z^2 = ax^2 + bxy + cy^2$ in $\mathbb{P}^2$, with $a = f_0$ and $b^2 - 4ac = \Delta(f)$ both nonzero in K. The pencil (A', B') has discriminant $f'(x,y) = ax^2y^2 + bxy^3 + cy^4$. Its base locus D in $\mathbb{P}^3$ is isomorphic to a singular curve of arithmetic genus one, with a single node R whose tangents are rational over the quadratic extension $K' = K(\sqrt{f_0})$. The Fano variety $F_{\mathfrak{m}}$ in this case is just the affine curve $D - \{R\}$, and $J^1_{\mathfrak{m}}$ is the affine curve $C_{\mathfrak{m}} - \{Q\} = C - \{P, P'\}$. Both are principal homogeneous spaces for the one-dimensional torus $T = J_{\mathfrak{m}}$ which is split by K'. We shall see that there is an unramified double cover $F_{\mathfrak{m}} \to J^1_{\mathfrak{m}}$ that extends to a double cover of complete curves of genus zero $M \to C$ which is ramified at P and P'.

Since the pencil is regular and its associated hyperelliptic curve has only nodal singularities, we again obtain a commutative algebraic group

$$X_{\mathfrak{m}} = J_{\mathfrak{m}} \sqcup F_{\mathfrak{m}} \sqcup J^1_{\mathfrak{m}} \sqcup F_{\mathfrak{m}} \tag{7}$$

over K with connected component $J_{\mathfrak{m}}$ and component group $\mathbb{Z}/4$. The group $X_{\mathfrak{m}}$ contains the algebraic group $\mathrm{Pic}_{C_{\mathfrak{m}}/K}/\mathbb{Z} \cdot d = J_{\mathfrak{m}} \sqcup J^1_{\mathfrak{m}}$ with index two [37, §3.2]. Just as in the generic case, multiplication by 2 in the group $X_{\mathfrak{m}}$ gives an unramified cover

$$F_{\mathfrak{m}} \to J^1_{\mathfrak{m}}$$

of degree 2^{2g+1} with an action of $J_{\mathfrak{m}}[2]$, and shows that $2[F_{\mathfrak{m}}] = [J^1_{\mathfrak{m}}]$ in the group $H^1(K, J_{\mathfrak{m}})$ of principal homogeneous spaces for $J_{\mathfrak{m}}$. Hence a necessary condition for the existence of such a pencil (A', B') is that the class of $J^1_{\mathfrak{m}}$ is divisible by 2. In this case, the necessary condition is also sufficient.

Theorem 24. *Let $f(x,y) = f_0x^{2g+2} + f_1x^{2g+1}y + \cdots + f_{2g+2}y^{2g+2}$ be a binary form of degree $2g+2$ over K with $\Delta(f)$ and f_0 both nonzero. Write $f(x,1) = f_0g(x)$ with $g(x)$ monic and separable. Let L be the étale algebra $K[x]/g(x)$ of degree n over K and let β denote the image of x in L. Let C be the smooth hyperelliptic curve of genus g with equation $z^2 = f(x,y)$ and let $C_{\mathfrak{m}}$ be the singular hyperelliptic curve of arithmetic genus $g+1$ with equation $z^2 = f(x,y)y^2$. Then the following conditions are all equivalent:*

a. There is a generic pencil (A, B) over K with $\mathrm{disc}(xA - yB) = f(x,y)$.

b. There is a regular pencil (A', B') over K with $\mathrm{disc}(xA' - yB') = f(x,y)y^2$.

c. The coefficient f_0 lies in the subgroup $K^{\times 2}N(L^\times)$ of $K^\times$.

d. The class of the homogeneous space $J^1_{\mathfrak{m}}$ is divisible by 2 in the group $H^1(K, J_{\mathfrak{m}})$.

e. The class of the homogeneous space $W_{\mathfrak{m}}[2]$ is in the image of the map $m'_2 : H^1(K, J_{\mathfrak{m}}[4]) \to H^1(K, J_{\mathfrak{m}}[2])$ induced by the multiplication by 2 map from $J_{\mathfrak{m}}[4]$ to $J_{\mathfrak{m}}[2]$.

f. There is an unramified two-cover of homogeneous spaces $F_{\mathfrak{m}} \to J^1_{\mathfrak{m}}$ for $J_{\mathfrak{m}}$ over K.

g. The maximal unramified abelian cover $U \to C - \{P, P'\}$ of exponent 2 over K^s descends to K.

h. The maximal abelian cover $M \to C$ of exponent 2 over K^s that is ramified only at the points $\{P, P'\}$ descends to K.

Note that the maximal abelian covers above all have degree 2^{2g+1}. The equivalence of conditions a, d, and f proves Theorem 13.

Proof. $c \Leftrightarrow a \Rightarrow b$. We have already seen the equivalence of a and c in Corollary 19. The implication $a \Rightarrow b$ is obvious from the construction of the regular pencil (A', B') from a generic pencil (A, B) earlier in this section.

$b \Rightarrow d \Leftrightarrow e \Leftrightarrow f$. When a regular pencil (A', B') over K with $\mathrm{disc}(xA' - yB') = f(x, y)y^2$ exists, the Fano variety $F_{\mathfrak{m}}$ of the base locus of this pencil provides a homogenous space for $J_{\mathfrak{m}}$ whose class is a square root of the class of $J^1_{\mathfrak{m}}$ in the group $H^1(K, J_{\mathfrak{m}})$. The equivalence of conditions d, e and f is clear.

$f \Rightarrow g \Rightarrow h$. Assuming that a two-cover $F \to J^1_{\mathfrak{m}}$ exists over K, we obtain the maximal unramified abelian cover of $C - \{P, P'\}$ by taking the fiber product with the morphism $C - \{P, P'\} \to J^1_{\mathfrak{m}}$, and the maximal abelian cover of C ramified only at the points $\{P, P'\}$ by taking the closure of the above unramified cover of $C - \{P, P'\}$.

$h \Rightarrow c$. Finally, assuming the existence of the maximal abelian cover $M \to C$ of exponent 2 that is ramified only at the points $\{P, P'\}$, we show that f_0 lies in the subgroup $K^{\times 2}N(L^\times)$ of $K^\times$, which will complete the proof of Theorem 24. The cover $M \to C$ corresponds to an inclusion of function fields $K(C) \to K(M)$. Over K^s, the function field $K^s(M)$ is obtained from $K^s(C)$ by adjoining the square roots of all rational functions on C whose divisors have the form $2d_1$ or $2d_1 + (P) + (P')$ for some divisor d_1 on C. Since the characteristic of K is not equal to 2, these square roots give either unramified covers of C or covers that are ramified only at the two points P and P' where the ramification is tame. More precisely, there are $2^{2g+1} - 1$ distinct quadratic extensions of $K^s(C)$ of this form that are contained in $K^s(M)$, and their composition is equal to $K^s(M)$.

Indeed, by Galois theory, these quadratic extensions correspond to the subgroups of index 2 in $J_{\mathfrak{m}}[2](K^s)$, or equivalently to nontrivial K^s-points in the Cartier dual $\mathrm{Res}_{L/K}\mu_2/\mu_2$. Let w be the rational function z/y^{g+1} on C, and let t be the rational function x/y on C, so $w^2 = f_0 g(t)$. The nontrivial points in $(\mathrm{Res}_{L/K}\mu_2/\mu_2)(K^s)$ correspond bijectively to the nontrivial monic factorizations $g(x) = h(x)j(x)$ over K^s, and the corresponding quadratic extension of $K^s(C)$ is given by $K^s(C)(\sqrt{h(t)}) = K^s(C)(\sqrt{j(t)})$. When both $h(x)$ and $j(x)$ have even degree, the divisors of the rational functions $h(t)$ and $j(t)$ are of the form $2d_1$ and the corresponding quadratic cover of the curve C is unramified. When the factors both have odd degree, these divisors are of the form $2d_1 + (P) + (P')$ and the quadratic cover is ramified at the points P and P'.

Since there might be no nontrivial factorizations of $g(x)$ over K, there might be no nontrivial K-rational points of $\mathrm{Res}_{L/K}\mu_2/\mu_2$ and hence no quadratic field extensions of $K(C)$ contained in $K(M)$. However, over L we have the factorization $g(x) = (x - \beta)j(x) = h(x)j(x)$, so the algebra $L(M)$ must contain a square root u of some constant multiple of the function $h(t) = (t - \beta)$. (The need to adjoin a square root of $t - \beta$ whose divisor has the form $2d_1 + (P) + (P')$ is the main reason for the appearance of the generalized Jacobian $J_{\mathfrak{m}}$ (cf. [28, Footnote 2]).) Write $u^2 = \alpha(t - \beta)$ with α in $L^\times$ and take the norm to $K(M)$ to obtain the equation $N(u)^2 = N(\alpha)g(t)$. Then the two rational functions $N(u)$ and w in $K(M)^\times$ have the same divisor, so they are equal up to a constant factor in $K^\times$. Writing $bN(u) = w$ with b in $K^\times$, we find $w^2 = b^2N(u)^2 = b^2N(\alpha)g(t)$. However, $w^2 = f_0 g(t)$, so $f_0 = b^2N(\alpha)$ is in the subgroup $K^{\times 2}N(L^\times)$ of $K^\times$. This completes the proof of Theorem 24. □

In fact, the obstruction classes for the eight conditions in Theorem 24 are all equal. More precisely, the obstruction class for conditions a, b, c is the class of f_0 in $K^\times/(K^{\times 2}N(L^\times))$. This group

can be viewed as a subgroup of $H^2(K, J_{\mathfrak{m}}[2])$ via

$$\operatorname{coker}\big(N : H^1(K, \operatorname{Res}_{L/K}\mu_2) \to H^1(K, \mu_2)\big) \hookrightarrow H^2(K, (\operatorname{Res}_{L/K}\mu_2)_{N=1}).$$

We denote the image of f_0 in $H^2(K, J_{\mathfrak{m}}[2])$ by $[f_0]$. This is the cohomological class d_f whose non-vanishing obstructs the existence of rational orbits with invariant binary form f for (all pure inner forms of) SL_n; see [6, §2.4 and Theorem 9]).

The obstruction class for conditions d, e is the class $\delta[J^1_{\mathfrak{m}}]$ in $H^2(K, J_{\mathfrak{m}}[2])$ where δ is the connecting homomorphism $H^1(K, J_{\mathfrak{m}}) \to H^2(K, J_{\mathfrak{m}}[2])$ arising from the exact sequence $1 \to J_{\mathfrak{m}}[2] \to J_{\mathfrak{m}} \xrightarrow{2} J_{\mathfrak{m}} \to 1$.

The obstruction class for conditions f, g, h comes from Galois descent. There is an unramified two-cover $\pi : J^1_{\mathfrak{m}} \to J^1_{\mathfrak{m}}$ over K^s obtained by identifying $J^1_{\mathfrak{m}}$ with $J_{\mathfrak{m}}$ using a K^s-point of $J^1_{\mathfrak{m}}$, then taking the multiplication-by-2 map on $J_{\mathfrak{m}}$. The descent obstruction of this cover to K is the image in $H^2(K, J_{\mathfrak{m}}[2])$ of the class $[\pi : J^1_{\mathfrak{m}} \to J^1_{\mathfrak{m}}]$ under the following map from the Hochschild-Serre spectral sequence:

$$H^0\left(K, H^1(C \times_K K^s - \{P, P'\}, J_{\mathfrak{m}}[2])\right) \longrightarrow H^2(K, J_{\mathfrak{m}}[2]).$$

This obstruction class equals $\delta[J^1_{\mathfrak{m}}]$ for formal reasons (cf. [33, Lemma 2.4.5]). We have the following strengthening of Theorem 24.

Theorem 25. *Let $f(x, y) = f_0x^{2g+2} + f_1x^{2g+1}y + \cdots + f_{2g+2}y^{2g+2}$ be a binary form of degree $2g + 2$ over K with $\Delta(f)$ and f_0 both nonzero. Let C be the smooth hyperelliptic curve of genus g with equation $z^2 = f(x, y)$ and let $J_{\mathfrak{m}}$ denote its generalized Jacobian. Then the obstruction classes for conditions a through h in Theorem 24 are all equal in $H^2(K, J_{\mathfrak{m}}[2])$, i.e., $[f_0] = \delta[J^1_{\mathfrak{m}}]$.*

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & J_{\mathfrak{m}}[2] & \longrightarrow & J_{\mathfrak{m}} & \xrightarrow{2} & J_{\mathfrak{m}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{=} & & \\
1 & \longrightarrow & (J_{\mathfrak{m}} \sqcup J^1_{\mathfrak{m}})[2] & \longrightarrow & J_{\mathfrak{m}} \sqcup J^1_{\mathfrak{m}} & \xrightarrow{2} & J_{\mathfrak{m}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mu_2 & \xrightarrow{=} & \mu_2 & & & & .
\end{array}$$

Here the map $J_{\mathfrak{m}} \sqcup J^1_{\mathfrak{m}} \xrightarrow{2} J_{\mathfrak{m}}$ is given by $[D] \mapsto 2[D] - \deg([D]) \cdot d$. Theorem 25 follows from the following two results.

Proposition 26. *For any $a \in K$, there exists a class $[J^{1/2}_a] \in H^1(K, J_{\mathfrak{m}} \sqcup J^1_{\mathfrak{m}})$ such that $2[J^{1/2}_a] = [J^1_{\mathfrak{m}}]$ in $H^1(K, J_{\mathfrak{m}})$ and such that the image of $[J^{1/2}_a]$ in $H^1(K, \mu_2) = K^\times/K^{\times 2}$ equals $f_0g(a) = f_0N_{L/K}(a - \beta)$.*

Lemma 27. *Let $1 \to A_1 \to B_1 \to C \to 1$ and $1 \to A_2 \to B_2 \to C \to 1$ be central extensions of algebraic groups over K such that the following diagram commutes:*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{=} & & \\
1 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & D & \xrightarrow{=} & D & & & &
\end{array}$$

Then the following diagram commutes up to sign:

$$\begin{array}{ccc} H^1(K, B_2) & \longrightarrow & H^1(K, C) \\ \downarrow & & \downarrow \\ H^1(K, D) & \longrightarrow & H^2(K, A_1) \end{array}$$

Lemma 27 follows from a direct cocycle computation. For more details, see [36, Lemma 2.8.2]. We note that when Lemma 27 is used to prove Theorem 25, all the cohomology groups are 2-torsion and hence commutativity up to sign is equivalent to commutativity. We now prove Proposition 26. Fix $a \in K$. Let $P_a \in C(K(\sqrt{\alpha}))$ be a point with x-coordinate a, where $\alpha = f_0 g(a)$, and let P'_a be the conjugate of P_a under the hyperelliptic involution. The class $[J^1_{\mathfrak{m}}] \in H^1(K, J_{\mathfrak{m}})$ is given by the 1-cocycle $\sigma \mapsto {}^{\sigma}(P'_a) - (P'_a)$. In other words,

$$[J^1_{\mathfrak{m}}]_\sigma = \begin{cases} 0 & \text{if } \sigma(\sqrt{\alpha}) = \sqrt{\alpha} \\ (P_a) - (P'_a) & \text{if } \sigma(\sqrt{\alpha}) = -\sqrt{\alpha}. \end{cases}$$

Let $[J_a^{1/2}]$ denote the following 1-cochain with values in $(J_{\mathfrak{m}} \sqcup J^1_{\mathfrak{m}})(K^s)$:

$$[J_a^{1/2}]_\sigma = \begin{cases} 0 & \text{if } \sigma(\sqrt{\alpha}) = \sqrt{\alpha} \\ (P_a) & \text{if } \sigma(\sqrt{\alpha}) = -\sqrt{\alpha}. \end{cases}$$

Since $2(P_a) - d = 2(P_a) - ((P_a) + (P'_a)) = (P_a) - (P'_a)$, we see that $2[J_a^{1/2}]_\sigma = [J^1_{\mathfrak{m}}]_\sigma$ for all $\sigma \in \mathrm{Gal}(K^s/K)$. Moreover, a direct computation shows that $[J_a^{1/2}]$ is a 1-cocycle and its image in $H^1(K, \mu_2)$ is the 1-cocycle $\sigma \mapsto {}^{\sigma}\sqrt{\alpha}/\sqrt{\alpha}$. This completes the proof of Proposition 26, and thus Theorem 25. □

6 Soluble orbits

In the previous section, we gave necessary and sufficient conditions for the existence of pencils of bilinear forms $(A, B) \in K^2 \otimes \mathrm{Sym}_2 K^n$ having a given invariant binary form. In this section, we consider *soluble* pencils of bilinear forms (A, B), i.e., those for which the associated Fano variety $F = F(A, B)$ has a K-rational point.

Fix a binary form $f(x, y)$ of degree $n = 2g + 2$ over K with $\Delta(f)$ and f_0 nonzero in K, and let C be the smooth hyperelliptic curve with equation $z^2 = f(x, y)$. Suppose that (A, B) is a generic pencil of bilinear forms on W over K with invariant binary form $f(x, y) = \mathrm{disc}(Ax - By)$ and let (A', B') be the regular pencil of bilinear forms on $W \oplus K^2$ having invariant binary form $f(x, y)y^2$ constructed in Section 5. We say that (A, B) lies in a *soluble* orbit for SL_n if the Fano variety $F_{\mathfrak{m}}$ of the base locus of (A', B') has a K-rational point. Similarly, we say that the pencil (A, B) lies in a *soluble* orbit for SL_n / μ_2 if the Fano variety F of the base locus of (A, B) has a K-rational point. In this section, we classify the soluble orbits for SL_n and SL_n / μ_2.

Since we have constructed an unramified two-cover $F_{\mathfrak{m}} \to J^1_{\mathfrak{m}}$, a necessary condition for the existence of soluble orbits for SL_n is that $J^1_{\mathfrak{m}}(K)$ is nonempty. In this case, the group $J_{\mathfrak{m}}(K)$ acts simply transitively on the set of points $J^1_{\mathfrak{m}}(K)$.

Theorem 28. *Let $f(x,y)$ be a binary form of degree $n = 2g+2$ over K with $\Delta(f)$ and f_0 nonzero in K. Then soluble orbits for the action of $\mathrm{SL}_n(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ having invariant binary form $f(x,y)$ exist if and only if there is a K-rational divisor of odd degree on the curve $C : z^2 = f(x,y)$. In that case, they are in bijection with the elements of $J^1_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K)$.*

Proof. Suppose first that soluble orbits with invariant binary form $f(x,y)$ exist. Let (A,B) be in $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x,y)$ such that the Fano variety $F(A,B)_{\mathfrak{m}}$ of the associated regular pencil (A',B') in $W \oplus K^2$ has a rational point. The stabilizer of (A,B) in SL_n is isomorphic to $J_{\mathfrak{m}}[2]$ by Corollary 19 and Proposition 22. Since $H^1(K, \mathrm{SL}_n) = 1$, we see that the rational orbits with invariant binary form $f(x,y)$ are in bijection with the elements in the Galois cohomology group $H^1(K, J_{\mathfrak{m}}[2])$. This bijection depends on the choice of the initial soluble orbit (A,B) which maps to the trivial class in $H^1(K, J_{\mathfrak{m}}[2])$.

Explicitly, suppose the pair $(A_1,B_1) \in K^2 \otimes \mathrm{Sym}_2 K^n$ has invariant binary form $f(x,y)$ and corresponds to the class $c \in H^1(K, J_{\mathfrak{m}}[2])$. Let (A_1',B_1') be the associated regular pencil with Fano variety $F(A_1,B_1)_{\mathfrak{m}}$. Then as elements of $H^1(K,J_{\mathfrak{m}})[4]$, we have, up to sign[1], the formula

$$[F(A_1,B_1)_{\mathfrak{m}}] = [F(A,B)_{\mathfrak{m}}] + j'(c), \tag{8}$$

where j' denotes the natural map $H^1(K,J_{\mathfrak{m}}[2]) \to H^1(K,J_{\mathfrak{m}})[2]$ and the addition is taking place in $H^1(K,J_{\mathfrak{m}})$. Hence we see that $F(A_1,B_1)_{\mathfrak{m}}$ is the trivial torsor of $J_{\mathfrak{m}}$ if and only if c is in the Kummer image of $J_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K)$. Therefore, the set of soluble orbits with invariant binary form $f(x,y)$ forms a principal homogeneous space for the quotient group $J_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K)$. The choice of the fixed soluble orbit (A,B) trivializes this principal homogeneous space.

On the other hand, if $x \in F(A,B)_{\mathfrak{m}}(K)$ is any rational point, then the sum $x+x = 2x$ in the algebraic group $X_{\mathfrak{m}}$ in (7) gives a rational point of $J^1_{\mathfrak{m}}$ well-defined up to hyperelliptic conjugation (cf. Footnote 1). Hence $J^1_{\mathfrak{m}}(K)$ is nonempty. Therefore, the set $J^1_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K)$ is also in bijection with $J_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K)$.

To complete the proof of Theorem 28, it remains to show that if $J^1_{\mathfrak{m}}(K)$ is nonempty, then soluble orbits with invariant binary form $f(x,y)$ exist. We show this first in the special case where the curve $C_{\mathfrak{m}}$ has a non-singular K-rational point $Q = (x_0,1,z_0)$. Let $L = K[x]/f(x,1)$ denote as usual the étale algebra of rank n associated to $f(x,y)$ and let β denote the image of x in L. The rational orbit corresponding to (Q) is given by the equivalence class of a pair (α,s) (see Corollary 19) where $\alpha = (x-T)(Q)$. Here "$x-T$" is the descent map introduced by Cassels [12]:

$$J^1_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K) \to (L^\times/L^{\times 2})_{N \equiv f_0}.$$

We note that s is not uniquely determined when $W_{\mathfrak{m}}[2]$ is a nontrivial torsor of $J_{\mathfrak{m}}[2]$. In this case, the fibers of the above $x-T$ map also have size 2. From the definition of the bijection between the set of rational orbits and the set of equivalence classes of pairs (α,s) in Section 2, we see that if the orbit corresponding to a pair (α,s) is soluble, then the orbit corresponding to any pair (α',s') with $\alpha' = \alpha$ is also soluble.

Consider the two bilinear forms (A',B') on $L \oplus K^2$ given by

$$\begin{aligned} \langle(\lambda,a,b),(\mu,a',b')\rangle_{A'} &= (\text{coefficient of } \beta^{n-1} \text{ in } \alpha\lambda\mu) + aa', \\ \langle(\lambda,a,b),(\mu,a',b')\rangle_{B'} &= (\text{coefficient of } \beta^{n-1} \text{ in } \alpha\beta\lambda\mu) + ab' + a'b. \end{aligned}$$

[1]The ambiguity of sign comes from the fact that we cannot distinguish between $[F_{\mathfrak{m}}]$ and $-[F_{\mathfrak{m}}]$ in $H^1(K,J_{\mathfrak{m}})$. In other words, we cannot distinguish the two copies of $F_{\mathfrak{m}}$ in the group $X_{\mathfrak{m}}$ defined in (7).

We show that for $\alpha = (x - T)(Q)$, there is a rational $(g+1)$-plane x' isotropic with respect to both bilinar forms.

When $z_0 \neq 0$, we have $\alpha = (x - T)(Q) = x_0 - \beta$. Then

$$x' = \mathrm{Span}\{(1,0,0), (\beta,0,0), \ldots, (\beta^{g-1},0,0), (\beta^g, 1, -\frac{1}{2}(x_0 + \frac{f_1}{f_0}))\}$$

is isotropic with respect to both bilinear forms. To check this, we note that the unique polynomial $P(x)$ of degree at most $2g+1$ with $P(\beta) = (x_0 - \beta)\beta^{2g+1}$ has leading coefficient $x_0 + f_1/f_0$.

When $z_0 = 0$, we set $h_0(t) = t - x_0$ and $h_1(t) = f(t,1)/(t - x_0)$. Then $\alpha = (x - T)(Q) = h_1(\beta) - h_0(\beta)$ and the following $(g+1)$-plane is isotropic with respect to both bilinear forms:

$$x' = \mathrm{Span}\{(h_1(\beta) - h_1(x_0), 0, 0), (\beta - x_0, 0, 0), \ldots, ((\beta - x_0)^{g-1}, 0, 0), ((\beta - x_0)^g, 1, -\frac{1}{2}((2g+1)x_0 + \frac{f_1}{f_0}))\}.$$

This can be checked by a simple calculation noting that $h_1(\beta)(h_1(\beta) - h_1(x_0)) = h_0(\beta)h_1(\beta) = 0$.

Before moving on to the general case, we make an important observation. Using this pencil with $\alpha = (x - T)(Q)$ as the base point, we obtain a bijection between the set of the rational orbits with invariant binary form $f(x,y)$ and $H^1(K, J_{\mathfrak{m}}[2])$ as described above. If (A_1, B_1) is an element of $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x,y)$ such that its associated α equals $(x - T)(D)$ for some $D \in J^1_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K)$, then the orbit of (A_1, B_1) corresponds to the class $D - (Q)$ or $D - (Q')$ in $J_{\mathfrak{m}}(K)/2J_{\mathfrak{m}}(K)$ where Q' denotes the hyperelliptic conjugate of Q. Hence the orbit of (A_1, B_1) is soluble.

We now treat the general case, assuming only that $J^1_{\mathfrak{m}}(K)$ is nonempty. Now $C_{\mathfrak{m}}$ has a non-singular point Q defined over some extension K' of K of odd degree k. Let $D \in J^1_{\mathfrak{m}}(K)$ denote the divisor class of degree 1 obtained by taking the sum of the conjugates of Q and subtracting $\frac{k-1}{2}$ times the hyperelliptic class. We claim that the orbits corresponding to D are soluble thereby completing the proof of Theorem 28. To prove the claim, let (A, B) be an element of $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x,y)$ such that its associated α equals $(x - T)(D)$, and let $F(A,B)_{\mathfrak{m}}$ denote the Fano variety of the associated regular pencil. Since C has a point over K', we have seen that the K'-rational orbits (α, s) with $\alpha = (x - T)(Q)$ and hence with $\alpha = (x - T)(D)$ are soluble over K'. In other words, $F(A,B)_{\mathfrak{m}}(K')$ is nonempty. Thus, as an element of $H^1(K, J_{\mathfrak{m}})$, the class of $F(A,B)_{\mathfrak{m}}$ becomes trivial when restricted to $H^1(K', J_{\mathfrak{m}})$. A standard argument using the corestriction map shows that this class is killed by the degree k of K' over K. Since $F(A,B)_{\mathfrak{m}}$ is a torsor of $J_{\mathfrak{m}}$ of order dividing 4 and k is odd, we see that $F(A,B)_{\mathfrak{m}}$ must be the trivial torsor. □

The same argument also classifies the soluble orbits for SL_n / μ_2, provided that C has a K-rational divisor of odd degree. The descent map "$x - T$" gives a map of sets

$$J^1(K)/2J(K) \to (L^\times/(L^{\times 2}K^\times))_{N \equiv f_0}$$

and is either 2-to-1 or injective (depending on the triviality of the class $W[2]$ in $H^1(K, J[2])$). To see that there are no soluble orbits when C has no divisors of odd degree, we use the exact sequence of commutative algebraic groups [37, Corollary 3.22]:

$$1 \to T \to X_{\mathfrak{m}} \to X \to 1.$$

If $J^1_{\mathfrak{m}}(K)$ is empty but both $J^1(K)$ and $F(K)$ are nonempty, then the quotient of $X(K)$ by the image of $X_{\mathfrak{m}}(K)$ maps onto the component group $\mathbb{Z}/4\mathbb{Z}$ of X. On the other hand, this quotient injects into $H^1(K, T)$, which has exponent 2, a contradiction. Hence we have proved the following:

Theorem 29. *Let $f(x,y)$ be a binary form of degree $n = 2g+2$ over K with $\Delta(f)$ and f_0 nonzero in K. Then soluble orbits for the action of $(\mathrm{SL}_n/\mu_2)(K)$ having invariant binary form $f(x,y)$ exist if and only if there is a K-rational divisor of odd degree on the curve $C : z^2 = f(x,y)$. In that case, they are in bijection with the cosets of $J^1(K)/2J(K)$ and the group $J(K)/2J(K)$ acts simply transitively on the set of soluble orbits.*

7 Finite fields and archimedean local fields

In this section we consider the orbits for the action of $(\mathrm{SL}_n/\mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ when the base field K is a finite field or an archimedean local field. In particular, we compute the number of these orbits with a fixed invariant binary form $f(x,y)$.

7.1 Finite fields

Let K be a finite field of odd cardinality q. Let $f(x,y)$ be a binary form of even degree n over K with nonzero discriminant Δ and nonzero first coefficient f_0, and write $f(x,1) = f_0 g(x)$. We factor

$$g(x) = \prod_{i=1}^{m} g_i(x)$$

where $g_i(x)$ has degree d_i and is irreducible. Then L is the product of m finite fields L_i of cardinality q^{d_i}. Since finite fields have unique extensions of any degree, we see that either one of the L_i has odd degree over K or all of the L_i contain the unique quadratic extension of K. Therefore, $f(x,y)$ always has either an odd or an even factorization over K.

Since the norm map $L^\times \to K^\times$ is surjective, f_0 is always a norm. By Corollary 20, the number of $(\mathrm{SL}_n/\mu_2)(K)$-orbits with binary form $f(x,y)$ is: 2^m if all L_i have even degree and $n \equiv 0 \pmod 4$; 2^{m-1} if all L_i have even degree and $n \equiv 2 \pmod 4$; and 2^{m-2} if some L_i has odd degree over K. The size of the stabilizer equals the number of even factorizations of $f(x,y)$ over K. Hence the stabilizer has size given as follows: 2^m if all L_i have even degree and $n \equiv 0 \pmod 4$; 2^{m-1} if all L_i have even degree and $n \equiv 2 \pmod 4$; and 2^{m-2} if some L_i has odd degree over K. Therefore, the number of pairs $(A,B) \in K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x,y)$ is $|(\mathrm{SL}_n/\mu_2)(K)| = |\mathrm{SL}_n(K)|$. This agrees with [1, §3.3]. For the purpose of application in Section 12, the main ingredients that we need are the number of orbits and the fact that all the orbits with the same invariant binary form have the same number of elements.

By Lang's theorem, we have $H^1(K,J) = H^1(K,J_{\mathfrak{m}}) = 0$. Hence the Fano varieties F and $F_{\mathfrak{m}}$ associated to an orbit always have a K-rational point, and every orbit is soluble.

7.2 $\mathbb{R}$ and $\mathbb{C}$

We now classify the orbits over $K = \mathbb{R}$ and $K = \mathbb{C}$. Let $f(x,y)$ be a binary form of degree n over K with nonzero discriminant Δ and nonzero first coefficient f_0, and write $f(x,1) = f_0 g(x)$. Over $\mathbb{C}$ there is a single orbit with binary form $f(x,y)$.

In the case when $K = \mathbb{R}$, we factor

$$g(x) = \prod_{i=1}^{r_1} g_i(x) \prod_{j=1}^{r_2} h_j(x)$$

where each $g_i(x)$ has degree one while each $h_j(x)$ has degree two and is irreducible. Then the algebra L is the product of r_1 copies of $\mathbb{R}$ and r_2 copies of $\mathbb{C}$, with $r_1 + 2r_2 = n$. Note that r_1 has the same parity as n, so is always even. The quotient group $\mathbb{R}^\times/(\mathbb{R}^{\times 2}N(L^\times))$ is trivial unless $r_1 = 0$, in which case it has order 2. Just as in the case of finite fields, $f(x, y)$ always has either an odd or an even factorization over $\mathbb{R}$.

If the form f is negative definite, then there are no orbits having invariant binary form $f(x, y)$. Indeed, in this case $r_1 = 0$ and the leading coefficient f_0 is negative. Morever, the hyperelliptic curve C with equation $z^2 = f(x, y)$ has no real points, and the map $\mathrm{Pic}_{C/\mathbb{R}}(\mathbb{R}) \to \mathrm{Br}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ is surjective. The real divisor classes that are not represented by real divisors have degrees congruent to $g - 1$ modulo 2. When g is even, the Jacobian $J(\mathbb{R})$ is connected and every principal homogeneous space for J is trivial. In particular, J^1 has real points (which are not represented by real divisors of odd degree). When g is odd, the real points of the Jacobian $J(\mathbb{R})$ have two connected components, and J^1 is the unique nontrivial principal homogeneous space for J. The points in the connected component of $J(\mathbb{R})$ are the real divisor classes of degree zero that are represented by real divisors.

If f is not negative definite, then the element f_0 is a norm from $L^\times$ to $\mathbb{R}^\times$. Hence rational orbits exist. When $r_1 = 0$, so f is positive definite, there are two orbits if $n \equiv 0 \pmod 4$ and there is only one orbit if $n \equiv 2 \pmod 4$. In both cases, the real points of the hyperelliptic curve $C(\mathbb{R})$ and its Jacobian $J(\mathbb{R})$ are both connected and the orbits are all soluble.

If $r_1 > 0$, then the form f is indefinite and the number of orbits is 2^{r_1-2}. These orbits are in bijection with the equivalence classes of sign assignments to the r_1 real linear factors of $f(x, y)$ subject to the condition that the product of the signs matches the sign of the leading coefficient of $f(x, y)$ and where two sign assignments are equivalent if they are exactly the negative of each other. The hyperelliptic curve C with equation $z^2 = f(x, y)$ has $m = r_1/2$ connected components in its real locus, and $J(\mathbb{R})$ has 2^{m-1} connected components. Since the subgroup $2J(\mathbb{R})$ is equal to the connected component of $J(\mathbb{R})$, it follows that 2^{m-1} of these rational orbits with invariant binary form f are soluble.

The computation for the sizes of the stabilizers is similar to the finite field case. If $r_1 = 0$, then the size of the stabilizer is $2^{n/2}$ if $n \equiv 0 \pmod 4$ and is $2^{n/2-1}$ if $n \equiv 2 \pmod 4$. If $r_1 > 0$, then the size of the stabilizer is $2^{n/2+m-2}$ where again $m = r_1/2$.

8 Global fields and locally soluble orbits

In this section, we assume that K is a global field of characteristic not 2. Let $f(x, y)$ be a binary form of degree $n = 2g + 2$ over K with nonzero discriminant. Let $C : z^2 = f(x, y)$ denote the associated hyperelliptic curve. Recall that an element (A, B) of $K^2 \otimes \mathrm{Sym}_2 K^n$ (or its $(\mathrm{SL}_n/\mu_2)(K)$-orbit) with invariant binary form $f(x, y)$ is *locally soluble* if the associated Fano variety $F(A, B)$ over K has points over every completion K_ν. We wish to determine when rational orbits and locally soluble orbits for the action of $(\mathrm{SL}_n/\mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ exist. Theorem 24 gives a list of necessary and sufficient conditions for the existence of rational orbits over general fields. In this section, we assume that there exists a locally soluble two-cover of J^1 over K and that $\mathrm{Div}^1(C)$ is locally soluble. The main result is that these two conditions are sufficient for the existence of a rational orbit and indeed a locally soluble orbit with invariant binary form $f(x, y)$. The proof will be cohomological in nature using Theorem 24.

Recall the torsor $W[2]$ of $J[2]$ which consists of points $P \in J^1$ such that $2P = d$, where d is

the hyperelliptic class of C. The class of $W[2]$ in $H^1(K, J[2])$ maps to the class of J^1 in $H^1(K, J)[2]$. Since $J^1(K_\nu)$ is nonempty for all ν, we see that a priori $W[2]$ lies in the 2-Selmer subgroup $\mathrm{Sel}_2(J/K)$ of $H^1(K, J[2])$. Let $\pi : F_0 \to J^1$ denote a locally soluble two-cover of J^1 over K. Let $F_0[4]$ denote the torsor of $J[4]$ consisting of points $x \in F_0$ such that $\pi(x) \in W[2]$. Then the class of $W[2]$ equals $m_2(F_0[4])$ where we recall that $m_2 : H^1(K, J[4]) \to H^1(K, J[2])$ is the map induced by multiplication by 2 from $J[4]$ to $J[2]$. Since $F_0(K_\nu)$ is nonempty for all ν, the class of $F_0[4]$ is in the 4-Selmer subgroup $\mathrm{Sel}_4(J/K)$ of $H^1(K, J[4])$.

Conversely, suppose C is any hyperelliptic curve over K with locally soluble $\mathrm{Div}^1(C)$ such that $W[2]$ is divisible by 2 in $\mathrm{Sel}_4(J/K)$. Then a locally soluble two-cover of J^1 over K exists. Indeed, suppose $W[2] = m_2(F[4])$ for some $F[4] \in \mathrm{Sel}_4(J/K)$. Let F denote the principal homogeneous space of J whose class in $H^1(K, J)$ is the image of $F[4]$ in $H^1(K, J)[4]$. Then $2F = [J^1]$ and hence there exists a map $F \to J^1$ realizing F as a two-cover of J^1.

Theorem 30. *Suppose $C : z^2 = f(x, y)$ is a hyperelliptic curve over a global field K of characteristic not 2 such that C has a rational divisor of degree 1 locally everywhere and such that J^1 admits a locally soluble two-cover over K (equivalently, $W[2]$ is divisible by 2 in $\mathrm{Sel}_4(J/K)$). Then there exists $(A, B) \in K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x, y)$. That is, orbits for the action of $(\mathrm{SL}_n / \mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x, y)$ exist.*

Proof. Let $T = (\mathrm{Res}_{K'/K} \mathbb{G}_m)_{N=1}$ be the kernel of $J_{\mathfrak{m}} \to J$ as in (5), where $K' = K[x]/(x^2 - f_0)$. We will need the following properties about the cohomology of T:

1. $H^1(K_\nu, T) = K_\nu^\times / N K_\nu'^\times$ has exponent 2 for any local completion K_ν of K;
2. $H^1(K, T) = K^\times / N K'^\times$ satisfies the local-global principle since K'/K is cyclic when K' is a field and $H^1(K, T)$ is trivial when $K' \simeq K \oplus K$;
3. $H^2(K, T) = \mathrm{Br}(K')_{N=1}$ satisfies the local-global principle with respect to places of K;
4. The map $H^1(K_\nu, T) \to H^1(K_\nu, J_{\mathfrak{m}})$ is injective for any local completion K_ν of K since Div^1 is locally soluble.

Let ϕ, i, δ be defined by the following diagram arising as part of the long exact sequence in Galois cohomology:

$$\begin{array}{ccccccc} H^1(K,T) & \xrightarrow{i} & H^1(K,J_{\mathfrak{m}}) & \xrightarrow{\phi} & H^1(K,J) & \xrightarrow{\delta} & H^2(K,T) \\ \downarrow 2 & & \downarrow 2 & & \downarrow 2 & & \\ H^1(K,T) & \xrightarrow{i} & H^1(K,J_{\mathfrak{m}}) & \xrightarrow{\phi} & H^1(K,J) & & \end{array}$$

where the vertical maps are all multiplication by 2. Let $[F]$ be a locally trivial class in $H^1(K, J)$ such that $2[F] = [J^1]$. By Theorem 24, it suffices to show that the class $[J^1_{\mathfrak{m}}]$ is divisible by 2 in $H^1(K, J_{\mathfrak{m}})$.

Since $[F]$ is locally trivial, its image under δ is also locally trivial. Since $H^2(K, T)$ has the local-global principle, it follows that $\delta([F]) = 0$ and so $[F]$ is in the image of ϕ. Let $[F_{\mathfrak{m}}]$ denote a class in $H^1(K, J_{\mathfrak{m}})$ mapping to $[F]$ via ϕ. Since $\phi([F_{\mathfrak{m}}])$ is locally trivial, we see that $[F_{\mathfrak{m}}]$ locally is in the image of i. Since $H^1(K_\nu, T)$ has exponent 2 for every local completion of K, it follows that $2[F_{\mathfrak{m}}]$ is locally trivial.

Now both $2[F_{\mathfrak{m}}]$ and $[J^1_{\mathfrak{m}}]$ are locally trivial and map to $[J^1]$ under ϕ. We claim they are in fact equal. Indeed, their difference $2[F_{\mathfrak{m}}] - [J^1_{\mathfrak{m}}]$ is a locally trivial element of $H^1(K, J_{\mathfrak{m}})$ mapping to 0 under ϕ. Hence there exists some $c \in H^1(K,T)$ such that $2[F_{\mathfrak{m}}] - [J^1_{\mathfrak{m}}] = i(c)$. Since the ν-adic restrictions of i are all injective, it follows that c is locally trivial and hence trivial by the local-global principle of $H^1(K,T)$. This shows that $[J^1_{\mathfrak{m}}] = 2[F_{\mathfrak{m}}]$ is divisible by 2. □

Under the assumption that $\mathrm{Div}^1(C)$ is locally soluble, the existence of a locally soluble two-cover of J^1 is in fact equivalent to the existence of a locally soluble orbit for the action of $(\mathrm{SL}_n/\mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$. We will see that $\mathrm{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits. Therefore, every locally soluble two-cover of J^1 is isomorphic to the Fano variety $F(A,B)$ associated to the pencil of quadrics determined by some $(A,B) \in K^2 \otimes \mathrm{Sym}_2 K^n$. This also proves Theorem 14.

Theorem 31. *Suppose $C : z^2 = f(x,y)$ is a hyperelliptic curve over a global field K of characteristic not 2 such that $\mathrm{Div}^1(C)(K_\nu) \neq \varnothing$ for all places ν of K. Then locally soluble orbits for the action of $(\mathrm{SL}_n/\mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x,y)$ exist if and only if $W[2]$ is divisible by 2 in $\mathrm{Sel}_4(J/K)$, or equivalently J^1 admits a locally soluble two-cover over K. Furthermore, when these conditions are satisfied, the group $\mathrm{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits and this set is finite.*

Before proving Theorem 31, we note that the notion of locally soluble orbit is a tricky one. There could exist an integral binary quartic form $f(x,y)$ that has locally soluble orbits but no soluble orbits over $\mathbb{Q}$. For a specific example (suggested by John Cremona; see also [33, §8.1]), consider the elliptic curve E defined by the equation $y^2 = x^3 - 1221$. This curve has trivial Mordell-Weil group $E(\mathbb{Q}) = 0$ and Tate-Shafarevich group isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$. The binary quartic form $f(x,y) = 3x^4 - 12x^3y + 11xy^3 - 11y^4$ of discriminant $\Delta = -40252707 = -3^5 11^2 37^2$ corresponds to a class b in the Tate-Shafarevich group of E that is divisible by 2. Any of the elements c of order 4 in the Tate-Shafarevich group with $2c = b$ gives a locally soluble orbit with invariant binary form $f(x,y)$. The hyperelliptic curve $z^2 = f(x,y)$ is locally soluble but has no global points; hence, by Theorem 29, there is no soluble orbit having invariant binary form $f(x,y)$.

There are also examples where rational orbits exist but there are no locally soluble orbits. For example, consider the binary quartic form $f(x,y) = -x^4 + 2x^3y + 104x^2y^2 - 104xy^3 - 2764y^4$ of discriminant $\Delta = -2^8 571$. The associated quartic field L has discriminant $-2^4 571 = -9136$ and ring of integers $\mathbb{Z}[\theta]$, where θ is a root of the polynomial $F(t) = t^4 - 2t^2 + 2t - 3$. Since $F(1) = -2$, $F(0) = -3$, and $F(-1) = -6$, the element $\theta^3 - \theta$ in $L^\times$ has norm $-6^2 \equiv -1 = f_0$. So there are orbits over $\mathbb{Q}$ with this invariant binary quartic form. On the other hand, the hyperelliptic curve $C : z^2 = f(x,y)$ of genus one is a principal homogeneous space of order 2 for its Jacobian E, which is an elliptic curve with equation $y^2 + xy = x^3 - x^2 - 929x - 10595$ and prime conductor 571. This curve has trivial Mordell-Weil group $E(\mathbb{Q}) = 0$ and Tate-Shafarevich group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Hence $\mathrm{Sel}_2(E/\mathbb{Q})$ and $\mathrm{Sel}_4(E/\mathbb{Q})$ are both isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. The curve C represents one of the nontrivial locally trivial principal homogeneous spaces for E. Since its class is not in the image of multiplication by 2 from $\mathrm{Sel}_4(E/\mathbb{Q})$, there are no locally soluble orbits. (Thanks to John Cremona and Noam Elkies for help with computation in this example.)

Proof of Theorem 31: Suppose locally soluble orbits with invariant binary form $f(x,y)$ exist. We prove first that $\mathrm{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits with invariant binary form $f(x,y)$. Indeed, suppose that (A,B) is a rational pencil with Fano variety $F(A,B)$ and

invariant binary form $f(x,y)$. Any other rational pencil (A_1, B_1) with the same binary form corresponds to a class c in $H^1(K, J[2])$ that is in the kernel of the composite map $\gamma : H^1(K, J[2]) \to H^1(K, \mathrm{SL}_n/\mu_2) \hookrightarrow H^2(K, \mu_2)$ ([4, Proposition 1]). The map γ is cup product with the class $W[2] \in H^1(K, J[2])$ ([28, Proposition 10.3]). Let $F(A_1, B_1)$ denote the Fano variety associated to the pencil (A_1, B_1). Then one has, up to sign (cf. Footnote 1),

$$[F(A_1, B_1)] = [F(A, B)] + j(c), \tag{9}$$

where j denotes the natural map $H^1(K, J[2]) \to H^1(K, J)[2]$ and the addition is taking place in $H^1(K, J)$. Since the subgroup $J(K_\nu)/2J(K_\nu)$ of $H^1(K_\nu, J[2])$ maps to the trivial class in $H^1(K_\nu, \mathrm{SL}_n/\mu_2)$ for all places ν, the Hasse principle for the cohomology of the group SL_n/μ_2 shows that the subgroup $\mathrm{Sel}_2(J/K)$ of $H^1(K, J[2])$ also lies in $\ker\gamma$. It is then clear from (9) that if (A, B) is locally soluble, then $c \in \mathrm{Sel}_2(J/K)$ if and only if (A', B') is locally soluble. Hence $\mathrm{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits with invariant binary form $f(x,y)$. Since the 2-Selmer group is finite, the set of locally soluble orbits with invariant binary form $f(x,y)$ is also finite. Moreover, if (A, B) is locally soluble, then $F(A, B)$ gives a locally soluble two-cover of J^1 over K.

We now consider the sufficiency of the existence of a locally soluble two-cover of J^1 for the existence of locally soluble orbits. Let F denote the Fano variety corresponding to one rational orbit with invariant binary form $f(x,y)$. The existence of this rational orbit was the content of Theorem 30. Let $F[4]$ denote the lift of F to a torsor of $J[4]$ consisting of elements $x \in F$ such that $x+x+x+x = 0$ in the group X of four components defined in Theorem 23. Let $\iota : H^1(K, J[2]) \to H^1(K, J[4])$ denote the map induced from the inclusion of $J[2]$ inside $J[4]$. Then we have the following exact sequence:

$$H^1(K, J[2]) \xrightarrow{\iota} H^1(K, J[4]) \xrightarrow{m_2} H^1(K, J[2]). \tag{10}$$

We need to show that there exists a class $c \in H^1(K, J[2])$ such that $c \cup W[2] = 0$ and $F[4] + \iota(c) \in \mathrm{Sel}_4(J/K)$. Let d_0 be a class in $\mathrm{Sel}_4(J/K)$ such that $W[2] = m_2(d_0)$. Since $m_2(F[4] - d_0) = W[2] - W[2] = 0$, there exists an element $c_0 \in H^1(K, J[2])$ such that $\iota(c_0) = F[4] - d_0$ by the exact sequence (10). Then it suffices to show that

$$c_0 \cup W[2] = 0. \tag{11}$$

For ease of notation, we denote the above cup product by $e_2(c_0, W[2])$ since the cup product is induced from the Weil pairing e_2 on $J[2]$. Since $d_0 \in \mathrm{Sel}_4(J/K)$ is isotropic with respect to e_4, we have

$$e_2(c_0, W[2]) = e_4(F[4] - d_0, d_0) = e_4(F[4], d_0).$$

Fix a place ν and denote by $F[4]_\nu$, $d_{0,\nu}$, $e_{4,\nu}$ the ν-adic restrictions. Pick any $D_\nu \in J^1(K_\nu)$. Since F arises from a pencil of quadrics, we define

$$F[2]^{D_\nu} = \{x \in F : x + x = D_\nu\}.$$

The image of this torsor of $J[2]$ in $H^1(K_\nu, J[4])$ is the torsor

$$F[4]^{2D_\nu - d} = \{x \in F : x + x + x + x = 2D_\nu - d\},$$

where d denotes the hyperelliptic class as before. Therefore, as elements of $H^1(K_\nu, J[4])$, we have

$$F[4]_\nu - \iota_\nu(F[2]^{D_\nu}) = \delta_{4,\nu}(2D_\nu - d),$$

where $\delta_{4,\nu}$ is the Kummer map $J(K_\nu)/4J(K_\nu) \to H^1(K_\nu, J[4])$ and ι_ν is the ν-adic restriction of ι. Since $d_0 \in \mathrm{Sel}_4(K, J)$, we see that $d_{0,\nu}$ is in the image of $\delta_{4,\nu}$. Since $J(K_\nu)/4J(K_\nu)$ is isotropic with respect to $e_{4,\nu}$, we have

$$e_{4,\nu}(F[4]_\nu, d_{0,\nu}) = e_{4,\nu}(\iota_\nu(F[2]^{D_\nu}), d_{0,\nu}) = e_{2,\nu}(F[2]^{D_\nu}, W[2]_\nu). \tag{12}$$

Choosing a different $D_\nu \in J^1(K_\nu)$ changes $F[2]^{D_\nu}$ by an element of $J(K_\nu)/2J(K_\nu)$. As $J(K_\nu)/2J(K_\nu)$ is isotropic with respect to e_2, the value of $e_{2,\nu}(F[2]^{D_\nu}, W[2]_\nu)$ does not depend on the choice of D_ν. Theorem 31 then follows from the following general lemma.

Lemma 32. *Suppose K is any local field of characteristic not 2. Let $f(x, y)$ be a binary form of degree $2g+2$ with nonzero discriminant such that the associated hyperelliptic curve $C : z^2 = f(x, y)$ satisfies $\mathrm{Div}^1(C)(K) \neq \varnothing$. Suppose there is a rational orbit for the action of $(\mathrm{SL}_n/\mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant binary form $f(x, y)$, and let F denote the associated Fano variety. Then*

$$e_2(F[2], W[2]) = 0, \tag{13}$$

where $F[2]$ denotes any lift of F to a torsor of $J[2]$ using a point of $J^1(K)$.

Proof. The first key point is that if (13) holds for one rational orbit, then it holds for any rational orbit with the same invariant binary form. Indeed, if F' denotes the torsor of J coming from a different orbit, then $F' - F \in \ker \gamma$, where $\gamma : H^1(K, J[2]) \to H^2(K, \mu_2)$ is cup product with $W[2]$. In other words, $e_2(F' - F, W[2]) = 0$. Hence $e_2(F[2], W[2]) = e_2(F'[2], W[2])$.

The second key point is that since $\mathrm{Div}^1(C)(K) \neq \varnothing$, there exists a soluble orbit by Theorem 29. Let F denote the corresponding torsor arising from this soluble pencil. Then $F[2] \in J(K)/2J(K)$ and hence $e_2(F[2], W[2]) = 0$. □

This completes the proof of Theorem 31. □

We conclude by remarking that the natural generalization of the *fake 2-Selmer set* $\mathrm{Sel}_{2,\,\mathrm{fake}}(C)$ of C ([11]), namely the *fake 2-Selmer set* $\mathrm{Sel}_{2,\,\mathrm{fake}}(J^1)$ of J^1, is in natural bijection with the set of locally soluble orbits for the group $(\mathrm{SL}_n^{\pm}/\mu_2)(K)$, where $\mathrm{SL}_n^{\pm}$ denotes as before the subgroup of elements of GL_n with determinant ± 1. Using the group SL_n instead of $\mathrm{SL}_n^{\pm}$ allows us to "unfake" this fake Selmer set (cf. [35]).

9 Existence of integral orbits

The purpose of this section is to prove Theorem 15. More precisely, we prove:

Theorem 33. *Assume that $n \geq 2$ is even. Let $f(x, y)$ be a binary form of degree $n = 2g + 2$ with coefficients in $16^n\mathbb{Z}$ such that the hyperelliptic curve $C : z^2 = f(x, y)$ has locally soluble Div^1. Then every locally soluble orbit for the action of $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$ on $\mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$ with invariant binary form $f(x, y)$ has an integral representative, i.e., a representative in $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$.*

By Theorem 17 with $D = \mathbb{Z}$ and $\mathbb{Z}_p$, it suffices to find a representative over $\mathbb{Z}_p$ for every soluble orbit over $\mathbb{Q}_p$ with $f(x, y) \in \mathbb{Z}_p[x, y]$ since an ideal can be defined by giving its localization and its norm is always principal since $\mathbb{Z}$ is a PID. We begin by recalling from [1, §2] the construction of an integral orbit associated to a rational point on C, or a p-adically integral orbit associated to a p-adic

point on C. For this we recall some of the notations in Section 2. Without loss of generality, we may assume $f_0 \neq 0$. (By our convention, C being a hyperelliptic curve is equivalent to $\Delta(f) \neq 0$.) Write $f(x,1) = f_0 g(x)$ and let $L = \mathbb{Q}_p[x]/g(x)$ be the corresponding étale algebra of rank n over $\mathbb{Q}_p$. For $k = 1, 2, \ldots, n-1$, there are integral elements

$$\zeta_k = f_0\theta^k + f_1\theta^{k-1} + \cdots + f_{k-1}\theta$$

in L. Let R_f be the free $\mathbb{Z}_p$-submodule of L having $\mathbb{Z}_p$-basis $\{1, \zeta_1, \zeta_2, \ldots, \zeta_{n-1}\}$. For $k = 0, 1, \ldots, n-1$, let $I_f(k)$ be the free $\mathbb{Z}_p$-submodule of L with basis $\{1, \theta, \theta^2, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\}$. By Theorem 17, an integral orbit is an equivalence class of triples (I, α, s) where I is an ideal of R_f, $\alpha \in L^\times$, and $s \in K^\times$, such that $I^2 \subset \alpha I_f(n-3)$, $N(I) = s\mathbb{Z}_p$, and $N(\alpha) = s^2 f_0^{n-3}$. The rational orbit is given by the equivalence class of the pair (α, s).

By a change of variable, we may assume that we have an integral point $P = (0, 1, c)$ on the curve $z^2 = f(x,y)$ over $\mathbb{Z}_p$, so that the coefficient $f_n = c^2$ is a square. Then set $\alpha = \theta$, and we have

$$\theta I_f(n-3) = \mathrm{Span}_{\mathbb{Z}_p}\{c^2, \theta, \theta^2, \ldots, \theta^{n-2}, f_0\theta^{n-1}\}. \tag{14}$$

Let $I = \mathrm{Span}_{\mathbb{Z}_p}\{c, \theta, \theta^2, \ldots, \theta^{(n-2)/2}, \zeta_{n/2}, \ldots, \zeta_{n-1}\}$. Then it is easy to check that I is an ideal of R_f, $I^2 \subseteq \alpha I_f(n-3)$, and

$$N(I)^2 = N(\theta)N(I_f(n-3)) = [c/f_0^{(n-2)/2}]^2\mathbb{Z}_p.$$

Let $s = \pm c/f_0^{(n-2)/2}$ be such that (α, s) corresponds to the rational orbit determined by P. The triple (I, α, s) gives an integral orbit representing the soluble orbit given by P in $J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. We note that this association of an integral orbit to a $\mathbb{Q}$-rational point, and the paucity of integral orbits, was the key to the arguments of [1] showing that rational points are rare.

Given one such $f(x,y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$ with coefficients in $16\mathbb{Z}$, then $2^{4i} \mid f_0^{i-1}f_i$ for $i = 1, \ldots, n$. Therefore, Theorem 33 follows from the following proposition where the assumption on the coefficients is asymmetrical in contrast to Theorem 33:

Proposition 34. *Assume that $n \geq 2$ is even. Let $f(x,y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$ be a binary form of degree $n = 2g+2$ satisfying $f_0 \neq 0$ and $2^{4i} \mid f_0^{i-1}f_i$ for $i = 1, 2, \ldots, n$ such that the hyperelliptic curve $C : z^2 = f(x,y)$ has locally soluble Div^1. Then every locally soluble rational orbit for the action of $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$ on $\mathbb{Q}^2 \otimes \mathrm{Sym}_2\,\mathbb{Q}^n$ with invariant binary form $f(x,y)$ has an integral representative.*

Proof. We work over $\mathbb{Z}_p$ and give an explicit construction of the ideal I, in a manner similar to the one-point case shown above (cf. [1, §2]) and the corresponding statements in [5, Proposition 8.2] and [31, Proposition 2.9]. There are several important differences due to f_0 not being 1.

Define $g(x,y) = x^n + f_1x^{n-1}y + f_0f_2x^{n-2}y + \cdots + f_0^{n-1}f_ny^n$. Then $g(f_0x, y) = f_0^{n-1}f(x,y)$ and so $(f_0\theta, 1)$ is a root of g. The condition $2^{4i} \mid f_0^{i-1}f_i$, which is nontrivial only when $p = 2$, implies that if $a \in \mathbb{Q}_p$ is non-integral, then $a - f_0\theta \in L^\times$ lies in $L^{\times 2}\mathbb{Q}_p^\times$.

We claim that it suffices to consider classes in $J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ that can be represented by a Galois-invariant divisor of the form

$$D = (P_1) + (P_2) + \cdots + (P_m) - D^*, \tag{15}$$

such that:

1. The points $P_i = (a_i, b_i, c_i)$ are non-Weierstrass and non-infinite;
2. The effective divisor D^* is supported on points above ∞;
3. The positive integer m is odd with $m \leq g+1$;
4. For every $i = 1, \ldots, m$, scale a_i, b_i, c_i so that $b_i = 1$. Then $f_0 a_i$ is integral and the a_i's are distinct.

Since $\mathrm{Div}^1(C)(\mathbb{Q}_p) \neq \varnothing$, every $\mathbb{Q}_p$-rational divisor class can be represented by a rational divisor by Proposition 21. By [38, Lemma 3.8], every class in $J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ has the desired form satisfying conditions 1, 2, 3 except for the oddness of m. As remarked above, if $f_0 a_i$ is not integral, then $f_0 a_i - f_0\theta \in L^{\times 2}\mathbb{Q}_p^\times$ and so is $a_i - \theta$. Removing all the points P_i with $f_0 a_i$ non-integral gives a rational divisor D' that has the same image as D via the $x - T$ map from $J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ to $(L^\times/(L^{\times 2}\mathbb{Q}_p^\times))_{N=f_0}$. By Theorem 17, a triple (I, α, s) exists for D if and only if it exists for D'. We may impose the condition that the a_i's are all distinct since we are working modulo $2J(\mathbb{Q}_p)$.

We now show that we only need to consider the case m odd. If m is even, then it forces f_0 to be a square and so the points at infinity are rational. Let ∞ denote one of them. Since D has degree 1, we see that the degree of D^* is odd. Let x_0 be an element of $\mathbb{Z}_p$ to be chosen later and consider the change of coordinate $(x, y) \mapsto (x - x_0 y, y) \mapsto (-y, x - x_0 y)$. Let $\widetilde{f}(x, y)$ denote the new binary form, which is $\mathrm{SL}_2(\mathbb{Z}_p)$ equivalent to $f(x, y)$. Let $\widetilde{C}$ and $\widetilde{J}$ denote the new hyperelliptic curve and its Jacobian. Let $Q_1, \ldots, Q_m, Q_0 \in \widetilde{C}$ denote the images of $P_1, \ldots, P_m, \infty$. We pick x_0 so that none of the points Q_i are Weierstrass for $\widetilde{C}$. The divisor D becomes the divisor $\widetilde{D} = (Q_0) + \cdots + (Q_m) -$ points at infinity, up to $2\widetilde{J}(\mathbb{Q}_p)$. If integral orbits exist for $\widetilde{D}$, then applying the inverse of the above $\mathrm{SL}_2(\mathbb{Z}_p)$ transformation gives the desired integral orbits for D. There are $m+1$ non-Weierstrass and non-infinite points in $\widetilde{D}$ and so we are done if $m \leq g$.

Suppose now $m = g+1$ is even. Let $\widetilde{R}(x)$ be a polynomial of degree at most $g+1$ such that $\widetilde{R}(\widetilde{a}_i) = \widetilde{c}_i$ where $Q_i = (\widetilde{a}_i, 1, \widetilde{c}_i)$ for each $i = 0, \ldots, g+1$. Then $\widetilde{f}(x, 1) - \widetilde{R}(x)^2$ has degree at most $2g+2$ and vanishes at $\widetilde{a}_0, \ldots, \widetilde{a}_{g+1}$. So it has at most g other roots. This shows that $\widetilde{D}$ is rationally equivalent to a divisor of the form $(R_1) + \cdots + (R_{m'}) -$ points at infinity, with $m' \leq g$. If m' is odd, then we are done. If m' is even, then since m' is now at most g, we may apply the above construction to obtain a divisor D'' of the form $(S_1) + \cdots + (S_{m'+1}) -$ points at infinity, such that the existence of integral orbits is equivalent for D'', $\widetilde{D}$ and D.

Suppose now D is a divisor of the form (15) satisfying conditions 1–4. Define $P(x) = (x - f_0 a_1) \cdots (x - f_0 a_m)$. By our assumption on the integrality of $f_0 a_i$, $P(x)$ is an integral polynomial. Write $\alpha_0 = (a_1 - \theta) \cdots (a_m - \theta)$. Then $P(f_0\theta) = -f_0^m \alpha_0$. Next define $R(x)$ to be a polynomial of degree at most $m-1$ so that $R(f_0 a_i) = f_0^{n/2} c_i$ for each $i = 1, \ldots, m$. Then $R(x)^2 - f_0 g(x, 1)$ vanishes at $f_0 a_1, \ldots, f_0 a_m$. So there exists an integral polynomial $h(x)$ such that $R(x)^2 - f_0 g(x, 1) = P(x)h(x)$. Note we have $R(f_0\theta)^2 = P(f_0\theta)h(f_0\theta)$.

Suppose first $R(f_0 x)$ is an integral polynomial. Then we set I_D to be the following R_f-submodule of L:

$$I_D = \langle f_0^{2m} R(f_0\theta), P(f_0\theta) I_f(\frac{n-3-m}{2}) \rangle.$$

Computing its square gives:

$$\begin{aligned} I_D^2 &= P(f_0\theta)\cdot\langle f_0^{4m}h(f_0\theta), f_0^{2m}R(f_0\theta)I_f(\frac{n-3-m}{2}), P(f_0\theta)I_f(n-3-m)\rangle \\ &= P(f_0\theta)f_0^m\cdot\langle f_0^{3m}h(f_0\theta), f_0^mR(f_0\theta)I_f(\frac{n-3-m}{2}), (\theta-a_1)\cdots(\theta-a_m)I_f(n-3-m)\rangle \\ &\subset f_0^{2m}\alpha_0 I_f(n-3). \end{aligned}$$

The last containment follows from computing the degrees of h and R. (When $m=1$, one checks directly that $h\in I(n-3)$.) We then set $\alpha = f_0^{2m}\alpha_0$ to get $I^2\subset \alpha I(n-3)$.

To compute the norm of I_D, we use a specialization argument. Let $\mathcal{R}$ denote the ring

$$\mathcal{R} = \mathbb{Z}_p[f_0,\ldots,f_n,a_1,\ldots,a_m][\sqrt{f(a_1,1)},\ldots,\sqrt{f(a_m,1)}],$$

where $f(x,1) = f_0x^n + f_1x^{n-1} + \cdots + f_n$. Write $c_i = \sqrt{f(a_i,1)}$ for each $i=1,\ldots,m$. Inside $\mathcal{R}[x]/f(x,1)$, we define $\zeta_1,\ldots,\zeta_{n-1}$ as before and denote the corresponding R_f, I_f, I_D by $\mathcal{R}_f, \mathcal{I}_f, \mathcal{I}_D$. One has the notion of $N\mathcal{I}_D$ as an $\mathcal{R}$-submodule of the fraction field of $\mathcal{R}$.

We claim that $N\mathcal{I}_D$ is the principal ideal generated by $s = c_1\cdots c_m f_0^{nm-(n-3+m)/2}$. Specializing to particular $f_0,\ldots,f_n,a_1,\ldots,a_m$ then completes the proof. We prove this claim by first inverting f_0. In this case, the result follows from [4, Proposition 8.5]. Next we localize at (f_0) to check that the correct power of f_0 is attained. Since every ideal is invertible now, it suffices to show that $\mathcal{I}_D^2 = \alpha\mathcal{I}_f^{n-3}$ which follows from the statements

$$(\theta-a_i)(\mathcal{R}_f)_{(f_0)} = (\mathcal{I}_f)_{(f_0)} \tag{16}$$

for $i=1,\ldots,m$. To prove (16), note that the containment $\subset$ is clear since $\theta-a_i\in\mathcal{I}_f$; equality follows because they have the same norm. We now give another more explicit proof of (16). Note that it remains to show that $1\in(\theta-a_i)(\mathcal{R}_f)_{(f_0)}$. Consider the polynomial $h_i(t) = (f(t,1)-c_i^2)/(t-a_i)$. By definition $h_i(\theta)(\theta-a_i) = -c_i^2$. Moreover, writing out $h_i(t)$ explicitly, one sees that

$$h_i(\theta) = \zeta_{n-1} + a_i\zeta_{n-2} + a_i^2\zeta_{n-3} + \cdots + a_i^{n-2}\zeta_1 + h_i(0)\in\mathcal{R}_f.$$

This shows that $c_i^2\in(\theta-a_i)(\mathcal{R}_f)_{(f_0)}$, and hence $1\in(\theta-a_i)(\mathcal{R}_f)_{(f_0)}$ since c_i is a unit in $(\mathcal{R}_f)_{(f_0)}$.

We now deal with the case when $R(f_0x)$ is not integral. The rational function $y-R(f_0x)/f_0^{n/2}$ vanishes at $P_1,\ldots,P_m$ which prompts us to consider the divisor $\mathrm{div}(y-R(f_0x)/f_0^{n/2})$, which amounts to studying the roots of $j(x) = f(x,1) - R(f_0x)^2/f_0^n$. Now $j(x)$ is a polynomial of degree n with leading coefficient f_0 since the degree of R^2 is at most $2m-2<n$. Since $R(f_0x)$ is not integral, $j(x)$ has a coefficient of valuation strictly less than $-n\nu_p(f_0)$, where ν_p denotes the p-adic valuation. Then $j(x)$ has at least $n-(2m-2)$ roots with valuation less than $-\frac{n+1}{n}\nu_p(f_0)$ as seen from its Newton polygon. In other words, $j(x)$ has at least $n-(2m-2)$ roots a_i^* such that $f_0a_i^*$ is not integral. These roots will then give a divisor that is divisible by 2 in $J(\mathbb{Q}_p)$. Since $j(x)$ vanishes at the x-coordinates of $P_1,\ldots,P_m$, we see that it has at most $m-2$ other roots a such that f_0a is integral. Hence $\mathrm{div}(y-R(f_0x)/f_0^{n/2})-D$ has the form $D'+E$ where D' has the form (15) with m replaced by $m'\le m-2$ and where $E\in 2J(\mathbb{Q}_p)$. If m' is even, then as we have shown above, there exists a divisor D'' of the form (15) with $m'+1<m$ non-Weierstrass non-infinite points. The proof now concludes by induction on m. Once $m=1$, the polynomial $R(f_0x)$ is integral. $\square$

In certain cases, we may show that a soluble rational orbit has a unique integral representative up to the action of $(\mathrm{SL}_n/\mu_2)(\mathbb{Z}_p)$:

Proposition 35. *Let p be any odd prime, and let $f(x,y) \in \mathbb{Z}_p[x,y]$ be a binary form of even degree n such that $p^2 \nmid \Delta(f)$ and $f_0 \neq 0$. Let C denote the hyperelliptic curve $z^2 = f(x,y)$. Suppose that $\mathrm{Div}^1(C)(\mathbb{Q}_p) \neq \varnothing$. Then the $(\mathrm{SL}_n/\mu_2)(\mathbb{Z}_p)$-orbits on $\mathbb{Z}_p^2 \otimes \mathrm{Sym}_2 \mathbb{Z}_p^n$ with invariant binary form $f(x,y)$ are in bijection with soluble $(\mathrm{SL}_n/\mu_2)(\mathbb{Q}_p)$-orbits on $\mathbb{Q}_p^2 \otimes \mathrm{Sym}_2 \mathbb{Q}_p^n$ with invariant binary form $f(x,y)$. Furthermore, if $(A,B) \in \mathbb{Z}_p^2 \otimes \mathrm{Sym}_2 \mathbb{Z}_p^n$ with invariant binary form $f(x,y)$, then $\mathrm{Stab}_{(\mathrm{SL}_n/\mu_2)(\mathbb{Z}_p)}(A,B) = \mathrm{Stab}_{(\mathrm{SL}_n/\mu_2)(\mathbb{Q}_p)}(A,B)$.*

Proof. As noted earlier, we only need to focus on the pair (I,α). The condition $p^2 \nmid \Delta(f)$ implies that the order R_f is maximal and that the projective closure $\mathcal{C}$ of C over $\mathrm{Spec}(\mathbb{Z}_p)$ is regular. By Theorem 29, the assumption that $\mathrm{Div}^1(C)(\mathbb{Q}_p) \neq \varnothing$ implies that soluble $\mathbb{Q}_p$-orbits with invariant binary form $f(x,y)$ exist. Since p is odd, the p-adic version of Proposition 34 implies that $\mathbb{Z}_p$-orbits with invariant binary form $f(x,y)$ exist. Therefore, by Remark 18, the set of equivalence classes of pairs (I,α) is nonempty and is in bijection with $(R_f^\times/(R_f^{\times 2}\mathbb{Z}_p^\times))_{N\equiv 1}$. Since the special fiber of $\mathcal{C}$ is geometrically reduced and irreducible, the Neron model $\mathcal{J}$ of its Jacobian $J_{\mathbb{Q}_p}$ is fiberwise connected ([10, §9.5 Theorem 1]) and its 2-torsion $\mathcal{J}[2]$ is isomorphic to $(\mathrm{Res}_{R/\mathbb{Z}_p}\mu_2)_{N=1}/\mu_2$. We have via étale cohomology ([31, Proposition 2.11]) that

$$\mathcal{J}(\mathbb{Z}_p)/2\mathcal{J}(\mathbb{Z}_p) \simeq (R_f^\times/(R_f^{\times 2}\mathbb{Z}_p^\times))_{N\equiv 1}.$$

The Néron mapping property implies that $\mathcal{J}(\mathbb{Z}_p)/2\mathcal{J}(\mathbb{Z}_p) = J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$.

For the stabilizer statement, we have $L^\times[2] = R_f^\times[2]$ which suffices when $n \equiv 2 \pmod 4$. When $n \equiv 0 \pmod 4$, the exact sequence (3) implies that it remains to compare $(L^{\times 2} \cap \mathbb{Q}_p^\times)/\mathbb{Q}_p^{\times 2}$ and $(R_f^{\times 2} \cap \mathbb{Z}_p^\times)/\mathbb{Z}_p^{\times 2}$. These two groups are nontrivial only when L contains a quadratic extension K' of $\mathbb{Q}_p$. Since $p^2 \nmid \Delta(f)$ and $n \geq 4$, the discriminant of the extension $K'/\mathbb{Q}_p$ cannot be divisible by p. Hence $K' = \mathbb{Q}_p(\sqrt{u})$ can only be the unramified quadratic extension of $\mathbb{Q}_p$. In other words, $u \in \mathbb{Z}_p^\times$. Hence in this case $(L^{\times 2} \cap \mathbb{Q}_p^\times)/\mathbb{Q}_p^{\times 2}$ and $(R_f^{\times 2} \cap \mathbb{Z}_p^\times)/\mathbb{Z}_p^{\times 2}$ both are equal to the group of order 2 generated by the class of u. □

10 The number of irreducible integral orbits of bounded height

Let $V = \mathrm{Sym}_2(W^*) \oplus \mathrm{Sym}_2(W^*)$ be the scheme of pairs of symmetric bilinear forms on W. Define the height $H(v)$ of an element $v \in V(\mathbb{Z})$ to be the height of its invariant binary form. We say that $v \in V(\mathbb{Z})$ is *irreducible* if its invariant binary form has nonzero discriminant. In [1, §4], the asymptotic number of irreducible $\mathrm{SL}_n^{\pm 1}(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ having height less than X was determined, and also the asymptotic number of such orbits whose invariant binary forms satisfy any finite set of congruences. The same computation applies also with $G = \mathrm{SL}_n/\mu_2$ in place of $\mathrm{SL}_n^{\pm 1}$. We assume henceforth that n is even.

To state this counting result precisely, recall from the discussion of Section 7.2 that we may naturally partition the set of elements in $V(\mathbb{R})$ with $\Delta \neq 0$ and whose invariant binary form is not negative definite into $\sum_{m=0}^{n/2} r(m)$ components, which we denote by $V^{(m,r)}$ for $m = 0, 1, \ldots, n/2$ and $r = 1, \ldots, r(m)$ where: $r(m) = 2^{2m-2}$ if $m \geq 1$; $r(0) = 2$ if $n \equiv 0 \pmod 4$; and $r(0) = 1$ if $n \equiv 2 \pmod 4$. A very similar partition is used in [1, §4.1.1].

For a given value of m, the component $V^{(m,r)}$ of $V(\mathbb{R})$ maps to the component $I(m)$ of non-negative definite binary n-ic forms in $\mathbb{R}^{n+1}$ having nonzero discriminant and $2m$ real linear factors. Let $\mathcal{F}^{(m,r)}$ denote a fundamental domain for the action of $G(\mathbb{Z})$ on $V^{(m,r)}$, and set

$$c_{m,r} = \mathrm{Vol}(\mathcal{F}^{(m,r)} \cap \{v \in V(\mathbb{R}) : H(v) < 1\});$$

here Vol denotes the Euclidean measure on $V(\mathbb{R})$. The number of r's that correspond to orbits soluble at $\mathbb{R}$ is $\#(J^1(\mathbb{R})/2J(\mathbb{R}))$ where J denotes the Jacobian of a hyperelliptic curve $z^2 = f(x,y)$ with $f(x,y) \in I(m)$. The size of this quotient does not depend on the choice of $f(x,y) \in I(m)$. Then from [1, Theorems 9 and 17], we obtain the following counting result:

Theorem 36. *Fix m, r. Suppose S is a $G(\mathbb{Z})$-invariant subset of $V(\mathbb{Z})^{(m,r)} := V(\mathbb{Z}) \cap V^{(m,r)}$ defined by finitely many congruence conditions modulo prime powers. Let $N(S;X)$ denote the number of $G(\mathbb{Z})$-equivalence classes of elements $v \in S$ satisfying $H(v) < X$. Then*

$$N(S;X) = c_{m,r} \cdot \prod_p \nu_p(S) \cdot X^{n+1} + o(X^{n+1}),$$

where $\nu_p(S)$ denotes the p-adic density of S in $V(\mathbb{Z})$.

11 Sieving to locally soluble orbits

Since local solubility is defined by infinitely many congruence conditions, we need a weighted version of Theorem 36 in which we allow weights to be defined by certain infinite sets of congruence conditions. The technique for proving such a result involves using Theorem 36 to impose more and more congruence conditions.

To describe which weight functions on $V(\mathbb{Z})$ are allowed, we need the following definition:

Definition 37. Suppose $U = \mathbb{A}^M$ is some affine space. A function $\phi : U(\mathbb{Z}) \to [0,1]$ is said to be *defined by congruence conditions* if there exist local functions $\phi_p : U(\mathbb{Z}_p) \to [0,1]$ satisfying the following conditions:

1. For all $v \in U(\mathbb{Z})$, the product $\prod_p \phi_p(v)$ converges to $\phi(v)$.
2. For each prime p, the function ϕ_p is locally constant outside some (p-adically) closed subset of $U(\mathbb{Z}_p)$ of measure 0.
3. The p-adic integral $\displaystyle\int_{U(\mathbb{Z}_p)} \phi_p(v)dv$ is nonzero.

A subset U' of $U(\mathbb{Z})$ is said to be *defined by congruence conditions* if its characteristic function is defined by congruence conditions.

Then we have the following theorem, which follows from Theorem 36 via a sifting argument just as in [7, §2.7].

Theorem 38. *Let $\phi : V(\mathbb{Z}) \to [0,1]$ be a $G(\mathbb{Z})$-invariant function that is defined by congruence conditions via local functions $\phi_p : V(\mathbb{Z}_p) \to [0,1]$. Fix m, r. Let S be a $G(\mathbb{Z})$-invariant subset of*

$V(\mathbb{Z})^{(m,r)}$ *defined by congruence conditions. Let* $N_\phi(S;X)$ *denote the number of* $G(\mathbb{Z})$*-equivalence classes of irreducible elements* $v \in S$ *having height bounded by* X*, where each equivalence class* $G(\mathbb{Z})v$ *is counted with weight* $\phi(v)$*. Then*

$$N_\phi(S;X) \leq c_{m,r} X^{n+1} \prod_p \int_{v \in V(\mathbb{Z}_p)} \phi_p(v)dv + o(X^{n+1}).$$

Identify the scheme of all binary n-ic forms over $\mathbb{Z}$ with $\mathbb{A}^{n+1}_{\mathbb{Z}}$ and let F_0 denote the set of all integral binary forms of degree n. If F is a subset of F_0, denote by $F(\mathbb{F}_p)$ the reduction modulo p of the p-adic closure of F in $\mathbb{A}^{n+1}_{\mathbb{Z}}(\mathbb{Z}_p)$.

Definition 39. A subset F of F_0 is *large* if the following conditions are satisfied:

1. It is defined by congruence conditions.
2. There exists a subscheme S_0 of $\mathbb{A}^{n+1}_{\mathbb{Z}}$ of codimension at least 2 such that for all but finitely many p, we have $F_0(\mathbb{F}_p)\backslash F(\mathbb{F}_p) \subset S_0(\mathbb{F}_p)$.

We identify hyperelliptic curves with their associated binary forms. We say that a family of hyperelliptic curves $z^2 = f(x,y)$ is *large* if the set of binary forms $f(x,y)$ appearing is large.

As an example, the subset F_1 of F_0 consisting of binary n-ic forms $f(x,y)$ such that the corresponding hyperelliptic curves C given by $z^2 = f(x,y)$ have locally soluble Div^1 is large. The set $F_2 \subset F_1$ of integral binary n-ic forms such that the corresponding hyperelliptic curves are locally soluble is also large. These two statements follow from [26, Lemma 15]. Our aim is to prove the analogue of Theorem 6 for all large families of hyperelliptic curves whose associated binary forms are contained in F_1.

Let F be a large subset of F_0 contained in F_1. Since the curves $z^2 = f(x,y)$ and $z^2 = \kappa^2 f(x,y)$ are isomorphic over $\mathbb{Q}$, where κ is the constant in Theorem 15, we assume without loss of generality that the coefficients of every $f(x,y)$ in F lie in $\kappa^2\mathbb{Z}$. To prove Theorem 6, we need to weigh each locally soluble element $v \in V(\mathbb{Z})$ whose invariant binary form is in F by the reciprocal of the number of $G(\mathbb{Z})$-orbits in the $G(\mathbb{Q})$-equivalence class of v in $V(\mathbb{Z})$. However, in order for our weight function to be defined by congruence conditions, we instead define the following weight function $w : V(\mathbb{Z}) \to [0,1]$:

$$w(v) := \begin{cases} \Big(\sum_{v'} \dfrac{\#\operatorname{Stab}_{G(\mathbb{Q})}(v')}{\#\operatorname{Stab}_{G(\mathbb{Z})}(v')}\Big)^{-1} & \text{if } v \text{ is locally soluble with invariant binary form in } F, \\ 0 & \text{otherwise,} \end{cases} \tag{17}$$

where the sum is over a complete set of representatives for the action of $G(\mathbb{Z})$ on the $G(\mathbb{Q})$-equivalence class of v in $V(\mathbb{Z})$. We then have the following theorem:

Theorem 40. *Let* F *be a large subset of* F_0 *contained in* F_1*. Moreover, suppose that the coefficients of every* $f(x,y) \in F$ *lie in* $16^n\mathbb{Z}$*. Then*

$$\sum_{\substack{C \in F \\ H(C)<X}} \#\operatorname{Sel}_2(J^1) \leq \sum_{m=0}^{n/2} \sum_{r \text{ soluble}} N_w(V(\mathbb{Z})_F^{(m,r)};X) + o(X^{n+1}), \tag{18}$$

where $V(\mathbb{Z})_F^{(m,r)}$ *is the set of all elements in* $V(\mathbb{Z})^{(m,r)}$ *whose invariant binary forms lie in* F*, and "*r *soluble" is short for "every element of* $V(\mathbb{Z})_F^{(m,r)}$ *is soluble over* $\mathbb{R}$*".*

Proof. By Theorems 31 and 33, the left hand side is equal to the number of $G(\mathbb{Q})$-equivalence classes of elements in $V(\mathbb{Z})$ that are locally soluble, have invariant binary forms in F, and have height bounded by X. Given a locally soluble element $v \in V(\mathbb{Z})$ with invariant binary form in F, let $v_1, \dots, v_k$ denote a complete set of representatives for the action of $G(\mathbb{Z})$ on the $G(\mathbb{Q})$-equivalence class of v in $V(\mathbb{Z})$. Then

$$\sum_{i=1}^{k} \frac{w(v_i)}{\#\operatorname{Stab}_{G(\mathbb{Z})}(v_i)} = \Big(\sum_{i=1}^{k} \frac{\#\operatorname{Stab}_{G(\mathbb{Q})}(v)}{\#\operatorname{Stab}_{G(\mathbb{Z})}(v_i)}\Big)^{-1} \sum_{i=1}^{k} \frac{1}{\#\operatorname{Stab}_{G(\mathbb{Z})}(v_i)} = \frac{1}{\#\operatorname{Stab}_{G(\mathbb{Q})}(v)}. \tag{19}$$

When $\operatorname{Stab}_{G(\mathbb{Q})}(v)$ is trivial, which happens for all but negligibly many $v \in V(\mathbb{Z})$ by [1, Proposition 14], (19) simplifies to

$$\sum_{i=1}^{k} w(v_i) = 1. \tag{20}$$

Since the size of $\operatorname{Stab}_{G(\mathbb{Q})}(v)$ is bounded above by 2^{2g}, (20) always holds up to an absolutely bounded factor. Therefore, the right hand side of (18) also counts the number of $G(\mathbb{Q})$-equivalence classes of elements in $V(\mathbb{Z})$ that are locally soluble, have invariant binary forms in F, and have height bounded by X. □

In order to apply Theorem 38 to bound $N_w(V(\mathbb{Z})^{(m,r)}; X)$, we need to know that w is defined by congruence conditions. The proof that w is indeed a product $\prod_p w_p$ of local weight functions is identical to the proof of [7, Proposition 3.6]. Therefore, to bound $N_w(V(\mathbb{Z})^{(m,r)}; X)$, it remains to compute $c_{m,r}$ and the p-adic integrals $\int w_p(v)dv$. We fix left-invariant top differentials $d\tau, d\mu$ on G and $\mathbb{A}_{\mathbb{Z}}^{n+1}$ defined over $\mathbb{Z}$ and denote by $\tau_\infty, \tau_p, \mu_\infty, \mu_p$ the induced measures on $G(\mathbb{R}), G(\mathbb{Q}_p), \mathbb{R}^{n+1}, \mathbb{Q}_p^{n+1}$ respectively. We normalize $d\mu$ such that μ_∞ is the usual Euclidean measure on $\mathbb{R}^{n+1}$ and $\mu_p(\mathbb{Z}_p^{n+1}) = 1$ for all primes p. Then, we have the following results:

$$\begin{aligned} c_{m,r}X^{n+1} &= \frac{|\mathcal{J}|\tau_\infty(G(\mathbb{Z})\backslash G(\mathbb{R}))}{\#J[2](\mathbb{R})}\mu_\infty(\{f \in I(m) | H(f) < X\}); \\ \int_{v\in V(\mathbb{Z}_p)} w_p(v)dv &= |\mathcal{J}|_p\tau_p(G(\mathbb{Z}_p))\mu_p(F_p)\frac{\#(J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p))}{\#J[2](\mathbb{Q}_p)}; \end{aligned}$$

here $\mathcal{J}$ is a nonzero rational constant; J denotes the Jacobian of any hyperelliptic curve defined by $z^2 = f(x, y)$ where $f(x, y) \in F \cap I(m)$; and F_p is the p-adic closure of F. The first equation is proved in [1, §4.4]. The second equation follows from the identical computation as in [31, §4.5].

For every place ν of $\mathbb{Q}$, we let a_ν denote the following quotient:

$$a_\nu = \frac{\#(J^1(\mathbb{Q}_\nu)/2J(\mathbb{Q}_\nu))}{\#J[2](\mathbb{Q}_\nu)}.$$

Because of the assumption that $J^1(\mathbb{Q}_\nu) \neq \varnothing$, this quotient depends only on ν, g. Indeed, it is equal to 2^{-g} for $\nu = \infty$, 2^g for $\nu = 2$, and 1 for all other primes (see, e.g., [4, Lemma 12.3]). The a_ν's satisfy the product formula $\prod_\nu a_\nu = 1$.

We now combine Theorem 38, Theorem 40, and the product formula $\prod_\nu |\mathcal{J}|_\nu = 1$ to obtain:

Theorem 41. *Let F be a large subset of F_0 contained in F_1. Moreover, suppose that the coefficients of every $f(x,y)$ in F lie in $16^n\mathbb{Z}$. Then*

$$\sum_{\substack{C\in F\\ H(C)<X}} \#\operatorname{Sel}_2(J^1) \le \sum_{m=0}^{n/2} \tau(G)\mu_\infty(\{f\in I(m)|H(f)<X\})\prod_p \mu_p(F_p) + o(X^{n+1}), \tag{21}$$

where $\tau(G)=2$ denotes the Tamagawa number of G.

12 Proofs of main theorems

All the results stated in the introduction, starting with Theorem 6, hold even if for each $g\ge 1$ we range over any large congruence family of hyperelliptic curves C over $\mathbb{Q}$ of genus g for which $\mathrm{Div}^1(C)$ is locally soluble. (See Definition 39 for the definition of "large".)

We prove Theorems 6 and 7 in this generality.

Proof of Theorem 6: Let F be a large family of hyperelliptic curves with locally soluble Div^1. Since Condition 2 in Definition 39 is a mod p condition, the Ekedahl sieve as in [2, Theorem 3.3] can be applied to obtain the following tail estimate.

Proposition 42. *Let F_p denote the p-adic closure of F in $\mathbb{Z}_p^{n+1}$. For any $M>0$, we have*

$$\#\bigcup_{p>M}\{f\in I(m)|f\notin F_p, H(f)<X\} = O(X^{n+1}/M)+O(X^n),$$

where the implied constant is independent of X and M.

Then by a sifting argument just as in [7, §2.7], we have

$$\sum_{\substack{C\in F\\ H(C)<X}} 1 = \sum_{m=0}^{n/2} \mu_\infty(\{f\in I(m)|H(f)<X\})\prod_p \mu_p(F_p) + o(X^{n+1}). \tag{22}$$

Dividing (21) by (22) gives Theorem 6. □

Proof of Theorem 7: Let F be a large family of hyperelliptic curves with locally soluble Div^1. Let $k>0$ be an odd integer. Recall that the 2-Selmer set of order k is defined to be the subset of elements of $\mathrm{Sel}_2(J^1)$ that locally everywhere come from points in $J^1(\mathbb{Q}_\nu)$ of the form $d_1-\frac{k-1}{2}d$ where d_1 is an effective divisor of degree k and d is the hyperelliptic class. To obtain the average size of this 2-Selmer set of order k, we need to perform a further sieve from the whole 2-Selmer set to this subset. Let $\varphi_\nu\le 1$ denote the local sieving factor at a place ν of $\mathbb{Q}$. Then to prove that the average size of the 2-Selmer set of order k is less than 2, it suffices to show that $\varphi_\nu<1$ for some ν.

We use the archimedean place. Suppose that $f(x,y)$ is a degree $2g+2$ binary form having $2m$ real linear factors with $m>0$ and let C be its associated hyperelliptic curve. Then $C(\mathbb{R})$ has m connected components and $J(\mathbb{R})/2J(\mathbb{R})$ has size 2^{m-1}. Let σ denote complex conjugation. Then for any $P\in C(\mathbb{C})$ with x-coordinate $t\in\mathbb{C}^\times$, we have that $(t-\beta)({}^\sigma t-\beta)=N_{\mathbb{C}/\mathbb{R}}(t-\beta)\in\mathbb{R}^{\times 2}$ for any $\beta\in\mathbb{R}$. Hence the descent "$x-T$" map sends the class of $(P)+({}^\sigma P)-d$ to 1 in $L^\times/L^{\times 2}\mathbb{R}$ where L

denotes the étale algebra of rank n associated to $f(x,y)$. Thus $(P)+({}^{\sigma}P)-d \in 2J(\mathbb{R})$. Therefore, the image of $(\mathrm{Sym}^k(C))(\mathbb{R})$ in $J^1(\mathbb{R})/2J(\mathbb{R})$ is equal to the image of $\mathrm{Sym}^k(C(\mathbb{R}))$ in $J^1(\mathbb{R})/2J(\mathbb{R})$. Since m is positive, C has a rational Weierstrass point over $\mathbb{R}$. Hence if $P \in C(\mathbb{R})$, then $2(P)-d \in 2J(\mathbb{R})$. Since $C(\mathbb{R})$ has m connected components, we see that the image of $\mathrm{Sym}^k(C(\mathbb{R}))$ in $J^1(\mathbb{R})/2J(\mathbb{R})$ has size at most

$$S_m(k) = \binom{m}{1} + \binom{m}{3} + \cdots + \binom{m}{k}.$$

There is a positive proportion of hyperelliptic curves $C : z^2 = f(x,y)$ in F such that $f(x,y)$ splits completely over $\mathbb{R}$. For any odd integer $k < g$, we have $S_{g+1}(k) < 2^g = |J^1(\mathbb{R})/2J(\mathbb{R})|$. Therefore, $\varphi_\infty < 1$.

Consider now the second statement that the average size of the 2-Selmer set of order k goes to 0 as g approaches ∞. We use the archimedean place again. Suppose that $f(x,y)$ is a degree $n = 2g+2$ binary form having $2m$ real linear factors and let C be its associated hyperelliptic curve. For a fixed odd integer $k > 0$, we have

$$\lim_{m\to\infty} \frac{S_m(k)}{|J^1(\mathbb{R})/2J(\mathbb{R})|} = \lim_{m\to\infty} \frac{S_m(k)}{2^{m-1}} = 0. \tag{23}$$

On the other hand, [15, Theorem 1.2] states that the density of real polynomials of degree n having fewer than $\log n/\log\log n$ real roots is $O(n^{-b+o(1)})$ for some $b > 0$. Therefore, the result now follows from this and (23). □

Our approach to Theorem 5 (which in turn implies Theorems 1 and 2), using a result of Dokchitser and Dokchitser (Appendix A), does not work in the generality of large families, but does work for "admissible" families as defined below.

Definition 43. A subset F of the set F_0 of all integral binary forms of degree n is *admissible* if the following conditions are satisfied:

1. It is defined by congruence conditions;
2. For large enough primes p, the p-adic closure of F contains all binary forms $f(x,y)$ of degree n over $\mathbb{Z}_p$ such that the hyperelliptic curve $z^2 = f(x,y)$ has a $\mathbb{Q}_p$-rational point.

We say that a family of hyperelliptic curves $z^2 = f(x,y)$ is *admissible* if the set of binary forms $f(x,y)$ appearing is admissible.

To prove Theorem 5 where we range over any admissible family of hyperelliptic curves over $\mathbb{Q}$ of genus $g \geq 1$ with locally soluble Div^1, we note that the result of Dokchitser and Dokchitser holds for admissible families (Theorem A.2). The rest of the proof is identical to that given in the introduction.

We conclude by giving a version of Theorem 1 in the most general setting that our methods allow.

Theorem 44. *Suppose F is a large congruence family of integral binary forms of degree $n = 2g+2$ for which there exist two primes p, q neither of which is a quadratic residue modulo the other such that the following conditions hold for a positive proportion of $f(x,y)$ in F:*

1. *The four integral binary forms $f(x,y)$, $pf(x,y)$, $qf(x,y)$, $pqf(x,y)$ all lie inside F and the hyperelliptic curves have points over $\mathbb{Q}_p$ and $\mathbb{Q}_q$.*

2. *If J denotes the Jacobian of the hyperelliptic curve $z^2 = f(x, y)$, then J has split semistable reduction of toric dimension 1 at p and good reduction at q.*

Then for a positive proportion of binary forms $f(x, y)$ in F, the corresponding hyperelliptic curve $C : z^2 = f(x, y)$ has no points over any odd degree extension of $\mathbb{Q}$ (i.e., the variety J^1 has no rational points), and moreover the 2-Selmer set $\mathrm{Sel}_2(J^1)$ is empty.

Appendix A: A positive proportion of hyperelliptic curves have odd/even 2-Selmer rank

by Tim and Vladimir Dokchitser

In this appendix we show that both odd and even 2-Selmer ranks occur a positive proportion of the time among hyperelliptic curves of a given genus.

For an abelian variety A defined over a number field K, write $\mathrm{rk}_2(A/K) = \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/K)$ for the 2-Selmer rank, and $\mathrm{rk}_{2^\infty}(A/K)$ for the 2^∞-Selmer rank[2]. We will say 'rank of a curve' meaning 'rank of its Jacobian'.

Theorem A.1. *The proportion of both odd and even 2^∞-Selmer ranks in the family of hyperelliptic curves over $\mathbb{Q}$,*

$$y^2 = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \qquad (n \geqslant 3),$$

ordered by height as in (2) is at least 2^{-4n-4}. In particular, assuming finiteness of the 2-part of Ш, at least these proportions of curves have Jacobians of odd and of even Mordell–Weil rank.

Theorem A.2. *Let K be a number field with ring of integers O. Fix $n \geqslant 3$. Consider the family of all hyperelliptic curves*

$$y^2 = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \qquad a_i \in \mathrm{O},$$

or any other "admissible" family (see Definition 43). Then a positive proportion of the hyperelliptic curves in the family, when ordered by height, have even 2-Selmer rank and a positive proportion have odd 2-Selmer rank. The same conclusion holds for the 2^∞-Selmer rank.

The proofs resemble that of [8, §4.1] for elliptic curves over $\mathbb{Q}$. Recall that the conjecture of Birch and Swinnerton-Dyer implies, in particular, that the parity of the rank of an elliptic curve E is determined by whether its root number — that is, the sign of the functional equation of the L-function $L(E, s)$ of E — is $+1$ or -1. The proof in [8] uses that twisting by -1 does not affect the height of the curve but often changes the root number, and that the parity of the Selmer rank is (unconjecturally) compatible with the root number.

This compatibility is not known for hyperelliptic curves (but see the forthcoming work of A. Morgan for 2-Selmer ranks for quadratic twists). Instead, we tweak the argument to use Brauer relations in biquadratic extensions, where it is known in enough cases. To illustrate the method, consider an elliptic curve $E/\mathbb{Q}$ with split multiplicative reduction at 2. Then it has root number -1 over $F = \mathbb{Q}(i, \sqrt{2})$, since the unique place above 2 in F contributes -1, while every other rational place

[2] Mordell–Weil rank + number of copies of $\mathbb{Q}_2/\mathbb{Z}_2$ in $Ш_{A/K}$; if Ш is finite, this is just the Mordell–Weil rank.

splits into an even number of places in F and so contributes $+1$. In other words, the sum of the Mordell–Weil ranks for the four quadratic twists

$$\mathrm{rk}(E/F) = \mathrm{rk}(E/\mathbb{Q}) + \mathrm{rk}(E_{-1}/\mathbb{Q}) + \mathrm{rk}(E_2/\mathbb{Q}) + \mathrm{rk}(E_{-2}/\mathbb{Q}) \qquad (*)$$

should be odd, and so both odd and even rank should occur among the 4 twists. The point is that for the 2^∞-Selmer rank, the parity in $(*)$ can be computed unconditionally, using a Brauer relation in $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{C}_2 \times \mathrm{C}_2$. Moreover, this works for general abelian varieties and over a general number field K, replacing $\mathbb{Q}(i, \sqrt{2})$ by a suitable biquadratic extension of K. The fact that most of the decomposition groups are cyclic allows us to avoid all the hard local computations and restrictions on the reduction types, and varying the curve in the family gives the required positive proportions.

The exact result we will use is:

Theorem A.3. *Let $F = K(\sqrt{\alpha}, \sqrt{\beta})$ be a biquadratic extension of number fields. Suppose that some prime $\mathfrak{p}_0$ of K has a unique prime above it in F. Let C/K be a curve with Jacobian J, such that*

1. *$C(K_{\mathfrak{p}_0}) \neq \varnothing$ and J has split semistable reduction of toric dimension 1 at $\mathfrak{p}_0$;*
2. *$C(K_{\mathfrak{p}}) \neq \varnothing$ and J has good reduction at $\mathfrak{p}$ for every $\mathfrak{p} \neq \mathfrak{p}_0$ that has a unique prime above it in F/K.*

Then

$$\mathrm{rk}_{2^\infty}(J/K) + \mathrm{rk}_{2^\infty}(J_\alpha/K) + \mathrm{rk}_{2^\infty}(J_\beta/K) + \mathrm{rk}_{2^\infty}(J_{\alpha\beta}/K) \equiv 1 \mod 2.$$

If, in addition, $C_\alpha(K_{\mathfrak{p}})$, $C_\beta(K_{\mathfrak{p}})$ and $C_{\alpha\beta}(K_{\mathfrak{p}})$ are non-empty for all primes $\mathfrak{p}$ of K that have a unique prime above them in F, then the same conclusion holds for the 2-Selmer rank as well.

Postponing the proof of this theorem, we first explain how it implies Theorems A.1 and A.2.

Proof of Theorem A.1

For Theorem A.1, it suffices to prove the following:

Proposition A.4. *Consider a squarefree polynomial $f(x) \in \mathbb{Q}[x]$,*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \qquad (n \geqslant 3,\ \ n = 2g+1 \text{ or } 2g+2),$$

whose coefficients satisfy $a_2 \equiv 1 \mod 8$, $a_{2g+1} \equiv 4 \mod 8$ and all other $a_i \equiv 0 \mod 8$. Then among the four hyperelliptic curves

$$y^2 = f(x), \qquad y^2 = -f(x), \qquad y^2 = 2f(x), \qquad y^2 = -2f(x)$$

at least one has even and at least one has odd 2^∞-Selmer rank.

Proof. Replacing $y \mapsto 2y + x$ in $C : y^2 = f(x)$ and dividing the equation by 4 yields a curve with reduction

$$\bar{C}/\mathbb{F}_2 : y^2 + xy = x^{2g+1}.$$

This equation has a split node at $(0,0)$ and no other singularities, so $\mathrm{Jac}(C)$ has split semistable reduction at 2 of toric dimension 1. Hensel lifting the non-singular point at ∞ on $\bar{C}$ we find that $C(\mathbb{Q}_2) \neq \varnothing$. Now apply Theorem A.3 with $K = \mathbb{Q}$, $F = \mathbb{Q}(i, \sqrt{2})$ and $\mathfrak{p}_0 = 2$. (Note that all odd primes split in $F/\mathbb{Q}$, and that $\mathrm{Jac}(C_\alpha) = (\mathrm{Jac}(C))_\alpha$.) □

Proof of Theorem A.2

Lemma A.5. *Let K be a finite extension of $\mathbb{Q}_p$ (p odd), with residue field $\mathbb{F}_q$. Take a hyperelliptic curve*

$$C : y^2 = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \qquad a_i \in \mathrm{O}_K,$$

and let $f(x) \in \mathbb{F}_q[x]$ be the reduction of the right-hand side.

1. *If f is squarefree of degree n and has an $\mathbb{F}_q$-rational root, then $\mathrm{Jac}(C)$ has good reduction, and $C_\alpha(K) \neq \varnothing$ for every $\alpha \in K^\times$.*
2. *If $f(x) = (x-a)^2 h(x)$ for some $a \in \mathbb{F}_q$ and some squarefree polynomial $h(x)$ of degree $n-2$ that possesses an $\mathbb{F}_q$-rational root and satisfies $h(a) \in \mathbb{F}_q^{\times 2}$, then $\mathrm{Jac}(C)$ has split semistable reduction of toric dimension 1, and $C_\alpha(K) \neq \varnothing$ for every $\alpha \in K^\times$.*
3. *If $f(x)$ is not of the form $\lambda h(x)^2$, $\lambda \in \mathbb{F}_q$, and $q > 4n^2$, then $C(K) \neq \varnothing$.*

Proof. In the first case, C has good reduction, and therefore so does $\mathrm{Jac}(C)$. In the second case, C has one split node and no other singular points, and so its Jacobian has split semistable reduction of toric dimension 1. In both cases, $f(x)$ has a simple root $b \in \mathbb{F}_q$, by assumption. Lifting it by Hensel's lemma, we get a point $(B, 0)$ on C/K. This point gives a K-rational point on every quadratic twist of C.

For (3), this is the argument in [26, Lemma 15]: write $f(x) = l(x)h(x)^2$ with l and h coprime and l non-constant and squarefree. By the Weil conjectures, the curve $y^2 = l(x)$ has at least $q + 1 - n\sqrt{q} > n$ rational points over $\mathbb{F}_q$. So there is at least one whose x-coordinate is not a root of f. It is non-singular on $y^2 = f(x)$, and by Hensel's lemma it lifts to a point in $C(K)$. □

Proof of Theorem A.2. Write O for the ring of integers of K, and $\mathbb{F}_\mathfrak{p}$ for the residue field at $\mathfrak{p}$.

Suppose we are given an admissible family $\mathcal{F}$ of hyperelliptic curves. In other words, for every prime $\mathfrak{p}$ the curves lie in some open set $\mathcal{F}_\mathfrak{p}$ of $\mathfrak{p}$-adic curves $C/\mathrm{O}_\mathfrak{p}$, defined by congruence conditions modulo $\mathfrak{p}^{m_\mathfrak{p}}$, and outside a finite set of primes Σ of O these sets include all curves with $C(\mathrm{O}_\mathfrak{p}) \neq \varnothing$. Enlarge Σ to include all primes $\mathfrak{p}|2$, with $m_\mathfrak{p}$ chosen so that units of the form $1 + p^{m_\mathfrak{p}}$ are squares in $\mathrm{O}_\mathfrak{p}$, and all primes of norm $\leqslant 4n^2$.

Take a prime $\mathfrak{p}_0 \notin \Sigma$. Pick $\alpha, \beta \in \mathrm{O}$ with $\alpha \equiv \beta \equiv 1 \mod \prod_{\mathfrak{p}\in\Sigma} \mathfrak{p}^{m_\mathfrak{p}}$, and such that α has valuation 1 at $\mathfrak{p}_0$ and β is a non-square unit modulo $\mathfrak{p}_0$. Then $\mathfrak{p}_0$ ramifies in $K(\sqrt{\alpha})$ and is inert in $K(\sqrt{\beta})$, so $F = K(\sqrt{\alpha}, \sqrt{\beta})$ is a biquadratic extension with a unique prime above $\mathfrak{p}_0$. There is a finite set of primes U of K that have a unique prime above them in F, and $U \cap \Sigma = \varnothing$. (The set is finite since such primes must ramify in F/K.)

Within our family $\mathcal{F}$ consider those curves $C : y^2 = f(x)$ whose reductions are as in Lemma A.5(2) at $\mathfrak{p}_0$, as in Lemma A.5(1) at all $\mathfrak{p} \in U \setminus \{\mathfrak{p}_0\}$, and such that $f \bmod \mathfrak{p}$ is not a unit times the square of a polynomial at any $\mathfrak{p} \notin \Sigma \cup U$. (This is a positive proportion of curves in $\mathcal{F}$ by [27].) For each such curve C, Theorem A.3 implies that both odd and even 2-Selmer ranks occur among the twists of $\mathrm{Jac}(C)$ by $1, \alpha, \beta$ and $\alpha\beta$, in other words the Jacobians of C, C_α, C_β and $C_{\alpha\beta}$. Note that these twists are in $\mathcal{F}$, since for $\mathfrak{p} \in \Sigma$ this twisting does not change the class modulo $\mathfrak{p}^{m_\mathfrak{p}}$, while for $\mathfrak{p} \notin \Sigma$ these twists are all locally soluble by Lemma A.5(3).

Because quadratic twists by α, β and $\alpha\beta$ only change the height by at most $N_{K/\mathbb{Q}}(\alpha\beta)^n$, we get the asserted positive proportion. □

Proof of Theorem A.3

We refer the reader to [18, §2] for the theory of Brauer relations and their regulator constants.

Notation A.6. Let F/K be a Galois extension of number fields with Galois group G, and A/K an abelian variety. Fix a global invariant exterior form ω on A/K. For $K \subset L \subset F$ and a prime p, we write

$Ш^{[p]}_{A/L}$	p-primary part of $Ш_{A/L}$ modulo divisible elements (a finite abelian p-group).
$\tilde{c}_{A/L}$	$\prod c_v \lvert\omega/\omega^o_v\rvert_v$, where the product is taken over all primes of L, c_v is the Tamagawa number of A/L at v, ω^o_v the Néron exterior form and $\lvert\cdot\rvert_v$ the normalised absolute value at v.

In the theorem below we write

$\mathcal{S}$	the set of self-dual irreducible $\mathbb{Q}_pG$-representations.
Θ	$= \sum n_i H_i$ a Brauer relation in G (i.e. $\sum_i n_i \operatorname{Ind}_{H_i}^G \mathbf{1} = 0$).
$\mathcal{C}(\Theta, \rho)$	the regulator constant $\prod_i \det\big(\frac{1}{\lvert H_i\rvert}\langle\,,\,\rangle\lvert\rho^{H_i}\big)^{n_i} \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, where $\langle\,,\,\rangle$ is some non-degenerate G-invariant pairing on ρ.

Finally, as in [17] we let[3]

$$\mathcal{S}_\Theta = \{\rho \in \mathcal{S} \mid \operatorname{ord}_p \mathcal{C}(\Theta, \rho) \equiv 1 \mod 2\}.$$

Theorem A.7. *Suppose A/K is a principally polarized abelian variety. For $\rho \in \mathcal{S}$ write m_ρ for its multiplicity in the dual p^∞-Selmer group of A/F. Then*

$$\sum_{\rho \in \mathcal{S}_\Theta} m_\rho \equiv \operatorname{ord}_p \prod_i \tilde{c}_{A/F^{H_i}} Ш^{[p]}_{A/F^{H_i}} \mod 2.$$

Proof. This is essentially [17, Thm. 1.6], except for the $Ш^{[p]}$ term in the right-hand side. For odd p, this term is a square and does not contribute to the formula. For $p = 2$, this is the formula that comes out of the proof of [17, Thm. 1.6]. There the main step of the proof ([17, Thm. 3.1]) assumes that A/K has a principal polarization induced by a K-rational divisor to get rid of the $Ш^{[2]}$ term coming from [17, Thm. 2.2]. □

Corollary A.8. *Let $F = K(\sqrt{\alpha}, \sqrt{\beta})$ be a biquadratic extension of number fields. For every principally polarized abelian variety A/K,*

$$\begin{aligned} &\operatorname{rk}_{2^\infty}(A/K) + \operatorname{rk}_{2^\infty}(A_\alpha/K) + \operatorname{rk}_{2^\infty}(A_\beta/K) + \operatorname{rk}_{2^\infty}(A_{\alpha\beta}/K) \equiv \\ (\dagger) \qquad &\equiv \operatorname{ord}_2 \frac{\tilde{c}_{A/K(\sqrt{\alpha})}\,\tilde{c}_{A/K(\sqrt{\beta})}\,\tilde{c}_{A/K(\sqrt{\alpha\beta})}}{\tilde{c}_{A/F}\,(\tilde{c}_{A/K})^2} \\ &\quad + \operatorname{ord}_2 \frac{\lvert Ш^{[2]}_{A/K(\sqrt{\alpha})}\rvert \lvert Ш^{[2]}_{A/K(\sqrt{\beta})}\rvert \lvert Ш^{[2]}_{A/K(\sqrt{\alpha\beta})}\rvert}{\lvert Ш^{[2]}_{A/F}\rvert \lvert Ш^{[2]}_{A/K}\rvert^2} \qquad \mod 2. \end{aligned}$$

Proof. Write $1, \mathrm{C}_2^a, \mathrm{C}_2^b, \mathrm{C}_2^c$ for the proper subgroups of $G = \operatorname{Gal}(F/K)$, and $\mathbf{1}, \epsilon_a, \epsilon_b, \epsilon_c$ for its 1-dimensional representations (so $\mathbb{C}[G/\mathrm{C}_2^\bullet] \cong \mathbf{1} \oplus \epsilon^\bullet$ for $\bullet = a, b, c$). Thus the four 2^∞-Selmer ranks in question are the multiplicities of these four representations in the dual 2^∞-Selmer group of A/F. Now apply the theorem to the Brauer relation

$$\Theta = \{1\} - \mathrm{C}_2^a - \mathrm{C}_2^b - \mathrm{C}_2^c + 2G. \tag{24}$$

[3] [17] also includes representations of the form $T \oplus T^*$ for some irreducible $T \not\cong T^*$ (T^* is the contragredient of T), but these have trivial regulator constants by [18, Cor. 2.25].

Its regulator constants are (see [18, 2.3 and 2.14])

$$\mathcal{C}_\Theta(\mathbf{1}) = \mathcal{C}_\Theta(\epsilon^a) = \mathcal{C}_\Theta(\epsilon^b) = \mathcal{C}_\Theta(\epsilon^c) = 2 \quad \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2},$$

and so $S_\Theta = \{\mathbf{1}, \epsilon_a, \epsilon_b, \epsilon_c\}$ in this case. □

Proof of Theorem A.3. We write the two expressions in $\mathrm{ord}_2(...)$ on the right-hand side of Corollary A.8 as a product of local terms. The modified Tamagawa numbers $\tilde{c}_{J/K}, \tilde{c}_{J/K(\sqrt{\alpha})}, \ldots$ are, by definition, products over primes of K, $K(\sqrt{\alpha})$, ..., and we group all terms by primes of K. Similarly, as shown by Poonen and Stoll in [26, §8], the parity of $\mathrm{ord}_2 Ш^{[2]}$ is a sum of local terms that are 1 or 0 depending on whether $\mathrm{Pic}^{g-1}(C)$ is empty or not over the corresponding completion, and again we group them by primes $\mathfrak{p}$ of K. This results in an expression

$$\mathrm{rk}_{2^\infty}(J/K) + \mathrm{rk}_{2^\infty}(J_\alpha/K) + \mathrm{rk}_{2^\infty}(J_\beta/K) + \mathrm{rk}_{2^\infty}(J_{\alpha\beta}/K) \equiv \sum_{\mathfrak{p}} t_{\mathfrak{p}} \mod 2.$$

There are three cases to consider for $\mathfrak{p}$:

If there are several primes $\mathfrak{q}_i|\mathfrak{p}$ in F, then the decomposition groups of $\mathfrak{q}_i$ are cyclic, and this forces $t_{\mathfrak{p}} = 0$. This is a general fact about Brauer relations and functions of number fields that are products of local terms, see [18, 2.31, 2.33, 2.36(l)].

If there is a unique prime $\mathfrak{q}|\mathfrak{p}$ in F, then $C(K_{\mathfrak{p}}) \neq \varnothing$ by assumption. So $\mathrm{Pic}^{g-1}(C)$ is non-empty in every extension of $K_{\mathfrak{p}}$, and all the local terms for $Ш^{[2]}$ above $\mathfrak{p}$ vanish. Also J has semistable reduction, again by assumption, so its Néron minimal model stays minimal in all extensions. The term $|\omega/\omega_v^o|_v$ always cancels in Brauer relations in this case, see e.g. [18, 2.29]. So the only contribution to $t_{\mathfrak{p}}$ comes from Tamagawa numbers.

When $\mathfrak{p} \neq \mathfrak{p}_0$, the Jacobian J has good reduction and the Tamagawa numbers are trivial, so $t_{\mathfrak{p}} = 0$. Finally, if $\mathfrak{p} = \mathfrak{p}_0$, then J has split semistable reduction at $\mathfrak{p}$ of toric dimension 1. In this case, the Tamagawa number term at $\mathfrak{p}$ multiplies to $2 \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, in other words $t_{\mathfrak{p}} = 1$. This follows e.g. from [18, 3.3, 3.23] for the Brauer relation (24). This proves the claim for the 2^∞-Selmer rank.

It remains to deduce the formula for rk_2 from the one for rk_{2^∞}. The difference between rk_2 and rk_{2^∞} comes from $Ш^{[2]}$ and the 2-torsion in the Mordell–Weil group on J, J_α, J_β, and $J_{\alpha\beta}$. Two-torsion is the same for all four twists, and so gives an even contribution. As for $Ш^{[2]}$, the local terms that define its parity give an even contribution at every prime of K that splits in F, as the twists then come in isomorphic pairs. At the non-split primes, all four twists have local points by assumption, and so the local terms are 0. □

Acknowledgments

We thank Jean-Louis Colliot-Thélène, John Cremona, Noam Elkies, Tom Fisher, Bjorn Poonen, Peter Sarnak, Arul Shankar, and Michael Stoll for many helpful conversations. The first and third authors were supported by a Simons Investigator Grant and NSF grant DMS-1001828, and the second author was supported by NSF grant DMS-0901102. The authors of the appendix were supported by Royal Society University Research Fellowships.

References

[1] M. Bhargava, Most hyperelliptic curves over $\mathbb{Q}$ have no rational points, http://arxiv.org/abs/1308.0395v1.

[2] M. Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials, http://arxiv.org/abs/1402.0031v1.

[3] M. Bhargava, J. Cremona, and T. Fisher, The density of hyperelliptic curves over $\mathbb{Q}$ of genus g that have points everywhere locally, preprint.

[4] M. Bhargava and B. Gross, Arithmetic invariant theory, http://arxiv.org/abs/1208.1007, *Lie Theory and Its Applications: Proceedings of the Conference in Honor of Nolan Wallach's* 70*th Birthday*, to appear.

[5] M. Bhargava and B. Gross, The average size of the 2 Selmer group of the Jacobians of hyperelliptic curves with a rational Weierstrass point, *Automorphic Representations and L-functions*, *TIFR Studies in Math.* **22** (2013), 23–91.

[6] M. Bhargava, B. Gross, and X. Wang, Arithmetic invariant theory II, http://arxiv.org/abs/1310.7689, *Progress in Mathematics, Representations of Lie Groups: In Honor of David A Vogan, Jr. on his 60th Birthday*, to appear.

[7] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, *Ann. of Math. (2)* **181** (2015), no. 1, 191–242.

[8] M. Bhargava and A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, *Ann. of Math. (2)* **181** (2015), no. 2, 587–621.

[9] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms, *Proc. London Math. Soc.* **s3-24** (1972), 385–394.

[10] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **21**, Berlin, New York: Springer-Verlag, 1990.

[11] N. Bruin and M. Stoll, Two-cover descent on hyperelliptic curves, *Math. Comp.* **78** (2009), no. 268, 2347–2370.

[12] J. W. S. Cassels, The Mordell-Weil group of curves of genus 2, *Arithmetic and Geometry I*, Birkhäuser, Boston (1983), 27–60.

[13] J.-L. Colliot-Thélène and B. Poonen, Algebraic families of nonzero elements of Shafarevich–Tate groups, *J. Amer. Math. Soc.* **13** (2000), no. 1, 83–99.

[14] J.-L. Colliot-Thélène and J. J. Sansuc, La descente sur les variétés rationnelles, II, *Duke Math. J.* **54** (1987), 375 – 492

[15] A. Dembo, B. Poonen, Q.-M. Shao, and O. Zeitouni, Random polynomials having few or no real zeros, *J. Amer. Math. Soc.* **15** (2002), 857–892.

[16] U. V. Desale and S. Ramanan, Classification of vector bundles of rank 2 on hyperelliptic curves, *Invent. Math.* **38** (1976), 161–185.

[17] T. Dokchitser and V. Dokchitser, Self-duality of Selmer groups, *Math. Proc. Cam. Phil. Soc.* **146** (2009), 257–267.

[18] T. Dokchitser and V. Dokchitser, Regulator constants and the parity conjecture, *Invent. Math.* **178**, no. 1 (2009), 23–71.

[19] R. Donagi, Group law on the intersection of two quadrics, *Annali della Scuola Normale Superiore di Pisa* **7** (1980), 217–239.

[20] N. N. Dong Quan, Algebraic families of hyperelliptic curves violating the Hasse principle. Available at `http://www.math.ubc.ca/~dongquan/JTNB-algebraic-families.pdf`.

[21] B. Gross, Hanoi lectures on the arithmetic of hyperelliptic curves, *Acta mathematic vietnamica* **37** (2012), 579–588.

[22] B. Gross, On Bhargava's representations and Vinberg's invariant theory, In: *Frontiers of Mathematical Sciences*, International Press (2011), 317–321.

[23] S. Lichtenbaum, Duality theorems for curves over p-adic fields, *Invent. Math.* **7**, (1969), 120–136.

[24] J. Milnor, *Introduction to Algebraic K-theory*, Princeton University Press and University of Tokyo Press, 1971.

[25] J. Nakagawa, Binary forms and orders of algebraic number fields, *Invent. Math.* **97** (1989), 219–235.

[26] B. Poonen and M. Stoll, The Cassels–Tate pairing on polarized abelian varieties, *Ann. of Math.* **150** (1999), 1109–1149.

[27] B. Poonen and M. Stoll, A local-global principle for densities, *Topics in number theory* (University Park, PA, 1997), 241–244, *Math. Appl.* **467**, Kluwer Acad. Publ., Dordrecht, 1999.

[28] B. Poonen and E. F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, *J. reine angew. Math.* **488** (1997), 141–188.

[29] M. Reid, The complete intersection of two or more quadrics, PhD Thesis, Trinity College, Cambridge (1972).

[30] J-P. Serre, *Groupes algébriques et corps de classes*, Hermann, 1959.

[31] A. Shankar and X. Wang, Average size of the 2-Selmer group for monic even hyperelliptic curves, `http://arxiv.org/abs/1307.3531`.

[32] S. Siksek, Chabauty for symmetric powers of curves, *Algebra & Number Theory* **3** (no. 2), 209–236.

[33] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics **114**, 2007.

[34] M. Stoll, Finite descent obstructions and rational points on curves, *Algebra and Number Theory* **1** (1997), 349–391.

[35] M. Stoll and R. van Luijk, Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$, *Acta Arithmetica* **159** (2013), 133–148.

[36] N. Thang, Weak Corestriction Principle for Non-Abelian Galois cohomology, *Homology, Homotopy and Applications* **5** (2003), 219–249.

[37] X. Wang, Maximal linear spaces contained in the base loci of pencils of quadrics, `http://arxiv.org/abs/1302.2385`.

[38] X. Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, Ph. D. thesis, Harvard University, 2013.

[39] M. Wood, Rings and ideals parametrized by binary n-ic forms, *J. London Math. Soc.* (2) **83** (2011), 208–231.

[40] M. Wood, Parametrization of ideal classes in rings associated to binary forms, *J. reine angew. Math.* **689** (2014), 169–199.